PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-083509
(43)Date of publication of application : 28.03.1997

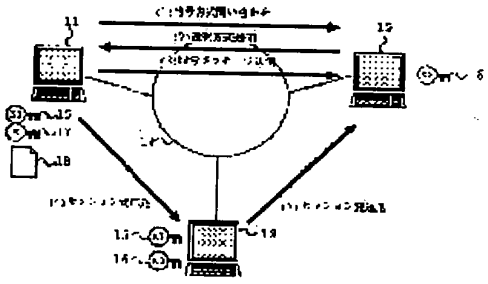
(51)Int.Cl. H04L 9/10
G06F 1/00
G06F 13/00
G09C 1/00
G09C 1/00
H04L 9/08
H04L 9/14
// H03M 7/40

(21)Application number : 07-234998
(22)Date of filing : 13.09.1995

(71)Applicant : HITACHI LTD
(72)Inventor : KAYASHIMA MAKOTO
TAKARAGI KAZUO
SUZAKI SEIICHI
NISHIOKA GENJI
TERADA MASATOSHI
YOSHIURA YUTAKA
UMEKI HISASHI

(54) CIPHER COMMUNICATION METHOD AND ITS DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To simplify the management of multiple common information different in specifications between a transmission-side computer and a reception-side computer, cryptographic keys, for example.
SOLUTION: A cipher or a compression algorithm used for ciphering a communication message between the transmission-side computer 11 and the reception-side computer 12 is negotiated and decided. A third computer 13 which can realize cipher or compression communication with the transmission-side computer 11 and the reception-side computer 12 by sharing information with the transmissions-side computer 11 and the reception-side computer 12 is arranged on a network. A session key for ciphering the communication message is ciphered by a common key between the transmissions-side computer 11 and the third computer 13 and is transmitted to the third computer 13. The third computer 13 reciphers the received session key by the common key with the reception-side computer 12 and transmits it to the reception-side computer 12. Thus, cipher communication with unspecified multiple opposite parties such as electronic transaction is realized and it is sufficient for both the transmission and reception computers to hold only a common key between the third computers. Thus, multiple common information different in specifications can be simplified.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The cryptocommunication approach characterized by to transmit the information used for encryption and compression-izing of a message or a message using said transmitting-side computer and said receiving-side computer, and the 3rd computer that can carry out cryptocommunication, respectively in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation.
[Claim 2] In the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation Said transmitting-side computer and said receiving-side computer, and the 3rd computer that can carry out cryptocommunication, respectively are arranged on a network. The cryptocommunication approach according to claim 1 characterized by enciphering a session key via the 3rd computer among the information used for encryption of a message, and transmitting.
[Claim 3] In the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation When a receiving-side computer receives the session key with which encryption which cannot be decrypted was performed, It is the cryptocommunication approach according to claim 1 which transmits the session key concerned to the 3rd computer, and is characterized by returning it to said receiving-side computer after processing the 3rd computer concerned so that said receiving-side computer can decrypt the session key concerned.
[Claim 4] The cryptocommunication approach according to claim 1 characterized by to encipher a message via the 3rd computer and to transmit when said transmitting-side computer and said receiving-side computer, and the 3rd computer that can communicate, respectively are arranged on a network in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation and a negotiation goes wrong.
[Claim 5] The cryptocommunication approach according to claim 1 characterized by determining the specification of a session key by the negotiation among the information used for encryption of a message in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation.
[Claim 6] The cryptocommunication approach according to claim 1 characterized by determining the information about compression of a message by the negotiation in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation.
[Claim 7] The cryptocommunication approach according to claim 2 characterized by to encipher using the common-use key shared in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation between the common-use key which shared encryption of a session key between a transmitting-side computer and the 3rd computer, and a receiving-side computer and the 3rd computer.
[Claim 8] The cryptocommunication approach according to claim 3 characterized by to encipher using the common-use key shared in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation between the common-use key which shared encryption of a session key between a transmitting-side computer and the 3rd computer, and a receiving-side computer and the 3rd computer.
[Claim 9] The cryptocommunication approach according to claim 2 characterized by giving the public key of the 3rd computer to a transmitting-side computer, giving the public key of a receiving-side computer to the 3rd computer, respectively, and enciphering encryption of a session key using said public key encryption in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation.

[Claim 10] The cryptocommunication approach according to claim 3 characterized by giving the public key of the 3rd computer to a transmitting-side computer, giving the public key of a receiving-side computer to the 3rd computer, respectively, and enciphering encryption of a session key using said public key encryption in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation.
[Claim 11] In the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation The cryptocommunication approach according to claim 4 characterized by enciphering using the common use key shared between the common use key shared between a transmitting-side computer and the 3rd computer, and a receiving-side computer and the 3rd computer to encryption of a message when a negotiation goes wrong.
[Claim 12] The cryptocommunication approach according to claim 4 characterized by giving the public key of the 3rd computer to a transmitting-side computer, giving the public key of a receiving-side computer to the 3rd computer at encryption of a message when a negotiation goes wrong in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation, respectively, and enciphering using said public key encryption.
[Claim 13] The cryptocommunication approach according to claim 5 characterized by determining the specification of a session key among the information used for encryption of a message using the path information between a transmitting-side computer and a receiving-side computer in the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network , and a receiving-side computer using the code or compression algorithm chosen by the negotiation .
[Claim 14] It is cryptocommunication equipment which is equipped with said transmitting-side computer and said receiving-side computer, and the 3rd computer in which cryptocommunication is possible respectively in the cryptocommunication equipment which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or the compression algorithm chosen by the negotiation, and is characterized by for said transmitting-side computer to transmit the information which uses for encryption and compression-izing of a message or a message through said 3rd computer.

[Claim 15] Cryptocommunication equipment according to claim 14 characterized by enciphering a session key via the 3rd [said] computer among the information which arranges on a network said transmitting-side computer and said receiving-side computer, and the 3rd computer that can carry out cryptocommunication, respectively, and is used for encryption of a message, and transmitting.
[Claim 16] It is cryptocommunication equipment according to claim 14 characterized by transmitting the session key concerned to said 3rd computer, and returning the 3rd computer concerned to said receiving-side computer after said receiving-side computer processes the session key concerned possible [a decryption] when said receiving-side computer receives the session key with which encryption which cannot be decrypted was performed.
[Claim 17] It is cryptocommunication equipment according to claim 14 characterized by enciphering a message via the 3rd computer and transmitting when said transmitting-side computer and said receiving-side computer, and the 3rd computer that can communicate, respectively are arranged on a network and said transmitting-side computer fails in said receiving-side computer and negotiation.
[Claim 18] Cryptocommunication equipment according to claim 14 characterized by determining the specification of a session key by the negotiation among the information used for encryption of a message.
[Claim 19] Cryptocommunication equipment according to claim 14 characterized by determining the information about compression of a message by the negotiation.
[Claim 20] Cryptocommunication equipment according to claim 15 characterized by enciphering using the common use key which shared encryption of a session key between the common use key shared between said transmitting-side computer and said 3rd computer, and said receiving-side computer and said 3rd computer.
[Claim 21] Cryptocommunication equipment according to claim 16 characterized by enciphering using the common use key which shared encryption of a session key between the common use key shared between said transmitting-side computer and said 3rd computer, and said receiving-side computer and said 3rd computer.
[Claim 22] Cryptocommunication equipment according to claim 15 characterized by giving the public key of said 3rd computer to said transmitting-side computer, giving the public key of said receiving-side computer to said 3rd computer, respectively, and enciphering encryption of a session key using said public key encryption.
[Claim 23] Cryptocommunication equipment according to claim 16 characterized by giving the public key of said 3rd computer to said transmitting-side computer, giving the public key of said receiving-side computer to said 3rd computer, respectively, and enciphering encryption of a session key using said public key encryption.
[Claim 24] Cryptocommunication equipment according to claim 17 characterized by enciphering using the common use key shared between the common use key shared between said transmitting-side computer and said 3rd computer, and said receiving-side computer and said 3rd computer to encryption of a message when a negotiation goes wrong.
[Claim 25] Cryptocommunication equipment according to claim 17 characterized by giving the public key of said 3rd computer to said transmitting-side computer, giving the public key of said receiving-side computer to said 3rd computer at encryption of a message when a negotiation goes wrong, respectively, and enciphering using said public

key encryption.
[Claim 26] Cryptocommunication equipment according to claim 18 characterized by determining the specification of a session key among the information used for encryption of a message using the path information between said transmitting-side calculating machines and said receiving-side calculating machines.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the cryptocommunication approach and equipment with which two or more transmitting origin or a transmission place exists especially with respect to the cryptocommunication approach and equipment which perform cryptocommunication between the transmitting-side computer linked to a network, and a receiving-side computer using the cryptographic algorithm chosen by the negotiation.
[0002]
[Description of the Prior Art] Conventionally, when it was the cryptocommunication system by which two or more transmitting origin and a transmission place exist, as for each computer, the share key needed to be managed for every transmission place. As an approach for mitigating this key management, the key management method based on the method of the following [the draft (ISO/IEC DIS 11770-2 Mechanism13) of ISO] is proposed.
[0003] (1) Arrange on a network the key management pin center,large which shares a transmission place and a reception place, and a key.
[0004] (2) Encipher with the key which is sharing encryption and a session key between the session key which generated the message at random between a transmitting side and a key management pin center,large, and send both to a receiving side.
[0005] (3) A receiving side sends the enciphered session key to a key management pin center,large.
[0006] (4) After a key management pin center,large decodes a session key, encipher with the key currently shared between a key management pin center,large and a receiving side, and send it to a receiving side.
[0007] Moreover, the cryptographic algorithm used for cryptocommunication needs to change the cryptographic algorithm used by the communications partner, when two or more transmitting origin and a transmission place exist. For this reason, it considers as the program interface which carries out the negotiation of the cryptographic algorithm used for cryptocommunication, and chooses it by the computers linked to a network, and the negotiation mechanism is proposed by GSS-API (Generic Security Service Application Program Interface). A GSS-API negotiation mechanism defines the outline of the following processings.
[0008] (1) Processing which notifies the cryptographic algorithm classification which the transmitting side is supporting to a receiving side.
[0009] (2) Processing which chooses an available thing from the cryptographic algorithm classification which the receiving side received, and is returned to a transmitting side.
[0010]
[Problem(s) to be Solved by the Invention] In case a commercial transaction etc. is performed using a network, in order to prevent a malfeasance, it is necessary to encipher a communication message. Usually, the method with which the cryptographic algorithm which enciphers a message serves as a criterion does not exist, but various kinds of methods are proposed. The encryption key used by cryptographic algorithm changes in the specification with algorithms. For example, in the case of DES, to the key length of an encryption key being 56 bits, when using MULTI, key length becomes 320 bits. For this reason, the computer which performs cryptocommunication among two or more transmission places needed to hold the cryptographic key of a different specification for every transmission place.
[0011] This invention aims at simplifying management of much share information between a transmitting-side computer and a receiving-side computer, for example, a share key, in the cryptocommunication system which performs cryptocommunication using the code or compression algorithm which had two or more transmission places, and was chosen by the negotiation between each transmission place.
[0012]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, in this invention, between the transmitting-side computer linked to a network, and a receiving-side computer In order to perform cryptocommunication in the cryptocommunication system which performs a code or a compression communication link using the code or compression algorithm chosen by the negotiation By sharing the share key 1 with a transmitting-side computer, a code, or a compression algorithm 1, and sharing a receiving-side computer, a code, or a compression algorithm 2 and its share key 2 Said transmitting-side computer and said receiving-side computer, and the 3rd computer that can perform a code or a compression communication link, respectively are arranged on a network. Processing which carries out the negotiation of the code or compression algorithm used for encryption of a message, and determines it between a transmitting-side calculating machine and a receiving-side calculating

machine is performed. By the transmitting-side calculating machine The processing which generates the additional information corresponding to the code or compression algorithm which carried out the negotiation, A message by the code or compression algorithm which carried out the negotiation, and said additional information Encryption or the processing which compression-izes and generates an encryption message, The processing which enciphers said additional information with said cryptographic algorithm 1 and the share key 1, and generates encryption additional information, Processing which transmits said encryption message to a receiving-side computer, and processing which transmits said encryption additional information to the 3rd computer are performed. By the 3rd computer The processing which decrypts the encryption additional information received from the transmitting-side computer with cryptographic algorithm 1 and the share key 1, and takes out additional information, The processing which enciphers with the cryptographic algorithm 2 which is sharing said additional information with a receiving-side computer, and the share key 2, and generates encryption additional information, Processing which transmits said encryption additional information to a receiving-side computer is performed. By the receiving-side computer The processing which decrypts the encryption additional information received from the 3rd computer with cryptographic algorithm 2 and the share key 2, and takes out additional information, It decrypts by the cryptographic algorithm which carried out the negotiation of the encryption message which received from the transmitting-side calculating machine, and said additional information, and processing which takes out a message is performed in order.

[0013] When the code between a transmitting-side computer and a receiving-side computer or the negotiation of a compression algorithm goes wrong, moreover, by the transmitting-side computer The processing which generates additional information applicable to the code or compression algorithm 1 currently shared with the 3rd computer, A message by cryptographic algorithm 1 and said additional information Encryption or the processing which compression-izes and generates an encryption message, The processing which enciphers said additional information with a code or a compression algorithm 1, and the share key 1, and generates encryption additional information, Processing which transmits said encryption message and encryption additional information to the 3rd computer is performed. By the 3rd computer The processing which decrypts the encryption additional information received from the transmitting-side computer with a code or a compression algorithm 1, and the share key 1, and takes out additional information, The processing which decrypts the encryption message which received from the transmitting-side calculating machine by the code or the compression algorithm 1, and said additional information, and takes out a message, The processing which generates additional information applicable to the code or compression algorithm 2 currently shared with a receiving-side computer, The processing which enciphers a message by the code or the compression algorithm 2, and said additional information, and generates an encryption message, The processing which enciphers said additional information with a code or a compression algorithm 2, and the share key 2, and generates encryption additional information, Processing which transmits said encryption message and encryption additional information to a receiving-side computer is performed. By the receiving-side computer The processing which decrypts the encryption additional information received from the 3rd computer with a code or a compression algorithm 2, and the share key 2, and takes out additional information, The encryption message which received from the 3rd calculating machine is decrypted by the code or the compression algorithm 2, and said additional information, and processing which takes out a message is performed in order.

[0014]

[Function] In the cryptocommunication system of this invention, cryptocommunication with many and unspecified partners like electronic commerce is made possible by carrying out the negotiation of the code or compression algorithm used for encryption of a message between a transmitting-side calculating machine and a receiving-side calculating machine. Furthermore, since a code or a compression communication link will be attained by arranging on a network a transmitting-side computer and a receiving-side computer, and the 3rd computer that shares a key, and transmitting additional information or a message via the 3rd computer according to the result of a negotiation if both of transmitting-side computers and receiving-side computers hold only the share information between the 3rd computer, management of much share information, for example, a share key, can be simplified.

[0015]

[Example] One example of this invention is explained using drawing 7 from drawing 1 . Drawing 1 is drawing showing the outline of the cryptocommunication system of this method. In 11, a transmitting-side computer reaches and, in 12, a receiving-side computer and 13 reach transmitting-side computer 11. The receiving-side computer 12, the 3rd computer which can communicate, and 14 The network between the transmitting-side computer 11, the receiving-side computer 12, and the 3rd computer 13, The encryption key which can apply 15 to the cryptographic algorithm 1 currently shared between the transmitting-side computer 11 and the 3rd computer 13, The encryption key which can apply 16 to the cryptographic algorithm 2 currently shared between the receiving-side computer 12 and the 3rd computer 13, the session key which generates 17 at random by the transmitting-side computer 11, and 18 are messages which transmit to the receiving-side computer 12 from the transmitting-side computer 11. In this system, the following procedure performs cryptocommunication between the transmitting-side computer 11 and the receiving-side computer 12.

[0016] (1) Ask the cryptographic algorithm method used for both cryptocommunication from the transmitting-side computer 11 to the receiving-side computer 12.

[0017] (2) The receiving-side computer 12 chooses the cryptographic algorithm method used for both cryptocommunication, and notifies it to the transmitting-side computer 11.

[0018] (3) The transmitting-side computer 11 generates the session key 17 which satisfies the requirements specified by the cryptographic algorithm notified from (a) receiving-side computer 12.

(b) Be with the session key 17, encipher an outgoing message 18 as the cryptographic algorithm notified from the receiving-side computer 12, and transmit to the receiving-side computer 12.
(c) Encipher with the cryptographic algorithm 1 which is sharing the session key 17 between the 3rd computer 13, and the encryption key 15, and transmit to the 3rd computer 13.
[0019] (4) The 3rd computer 13 decrypts the enciphered session key 17 which was received from (a) transmitting-side computer 11 using the cryptographic algorithm 1 and the encryption key 15 which are shared between the transmitting-side computers 11.
(b) Encipher with the cryptographic algorithm 2 which is sharing the decrypted session key 17 between the receiving-side computers 12, and the encryption key 16, and transmit to the receiving-side computer 12.
[0020] (5) The receiving-side computer 12 decrypts the enciphered session key 17 which was received from the (a) 3rd computer 13 using the cryptographic algorithm 2 and the encryption key 16 which are shared between the 3rd computer.
(b) Decrypt the enciphered message which was received from the transmitting-side calculating machine 11 using the cryptographic algorithm and the session key 17 which were decided by the negotiation.
here — the transmitting-side computer 11 and the receiving-side computer 12 — Huffman — the case where the compression algorithm by law is being supported — a message — Huffman — it can compress by law and the Huffman tree to the modulation code in a message can also be used as a session key.
[0021] Drawing 2 is drawing having shown the internal configuration of the computer used by this method. The flag of the cipher system which uses 21 for memory and uses 211 for session key generation, A data encryption key storage area and 213 212 A session key storage area, As for a bus and 23, the area which loads the code and decryption program corresponding to the cryptographic algorithm of various kinds [214 / 215 / a message storage area and], and 22 are [CPU and 24] external storage. The code and decryption program group for which 241 can use this computer, and 242 A session key generator, As for the database of the database about the specification of the key which uses 243 by the code and the decryption program group 241, the key which is sharing 244 among other calculating machines, and the cryptographic algorithm name used with the key, and 25, communication link I/O and 26 are the channels to other calculating machines.
[0022] Drawing 3 is drawing having shown the flow of processing with this method to the message at the time of a negotiation being successful. First, when it succeeds in the cipher system negotiation processing 301 which chooses the cryptographic algorithm used for the cryptocommunication between the receiving-side computers 12 by the transmitting-side computer 11, The session key creation processing 302 which creates the session key 17 suitable for the cryptographic algorithm determined by 301, The encryption processing 303 which enciphers a message 18 using the cryptographic algorithm and the session key 17 which were determined by 301, and generates a cipher 305, The session key 17 is enciphered using the cryptographic algorithm and the encryption key 15 which were decided beforehand between the 3rd computer 13. Perform encryption processing 304 which generates the enciphered session key 306, the enciphered session key 306 is transmitted to the 3rd computer 13, and a cipher 305 is transmitted to the receiving-side computer 12, respectively. By the 3rd computer 13, next, the enciphered session key 306 which was received from the transmitting-side computer 11 The cryptographic algorithm beforehand decided between the transmitting-side computers 11, and the decryption processing 307 decrypted using the encryption key 15, It enciphers using the cryptographic algorithm which determined beforehand the session key decrypted by 307 between the receiving-side computers 12, and the encryption key 16. Encryption processing 308 which generates the enciphered session key 309 is performed, and the enciphered session key 309 is transmitted to the receiving-side computer 12. Furthermore, by the receiving-side computer 12, cryptographic algorithm which determined beforehand the enciphered session key 309 which was received from the 3rd computer 13 between the 3rd computer 13, the decryption processing 310 which decrypts the session key 17 using the encryption key 16, and decryption processing 311 which decrypts a message 18 using the cryptographic algorithm which determined the cipher 305 received from the transmitting-side computer 11 by 301, and the session key 17 are performed.
[0023] Drawing 4 is the flow chart which showed processing of the transmitting-side calculating machine 11 in the cryptocommunication system of this method. The step which performs processing which 401 searchs a code and the decryption program group 241, and lists the usable cryptographic algorithm of the transmitting-side computer 11, The step which notifies the cryptographic algorithm name which listed 402 at step 401 to the receiving-side computer 12, 403 receives the cryptographic algorithm name which the receiving computer 12 chose. When the step set as the cipher system flag 211 for session keys and the cipher system for the cipher system flag 211 for session keys with suitable 404 are stored, The step which starts the session key generator 242, creates the session key 17 based on the key specification database 243, and is stored in the session key storage area 212, and the session key 17 which created 405 at step 405, Start the code and the decryption program 241 corresponding to the cipher system flag 211 for session keys, and a message 18 is enciphered. The step which generates a cipher 305, the step which transmits the cipher 305 which created 406 at step 405 to the receiving-side computer 12 by communication link I/O25, 407 reaches share encryption key 15 as the 3rd computer 13 stored in the key database 244. The session key 17 which started the code and the decryption program 241 corresponding to cryptographic algorithm, and was stored in the session key storage area 212 is enciphered. The step which stores the enciphered session key 306 in the session key storage area 212, and 408 are steps which transmit the enciphered session key 306 which was created at step 407 to the 3rd computer 13 by communication link I/O25.
[0024] Drawing 5 is the flow chart which showed the processing which chooses the cryptographic algorithm which

the receiving-side computer 12 in the cryptocommunication system of this method uses for session key 17 creation. The step which receives the cryptographic algorithm namelist to which 501 is sent from the transmitting-side computer 11, and the cryptographic algorithm namelist which 502 received at step 501, The step which compares the code and the decryption program group 241 of the receiving-side computer 12, The step cryptographic algorithm with 503 [available to the cipher system flag 211 for session keys] judges whether it is set up to be, The step at which 504 sets the name of the cryptographic algorithm common to both as the cipher system flag 211 for session keys, The step at which 505 sets NULL as the cipher system flag 211 for session keys, and 506 are steps which transmit the contents of the cipher system flag 211 for session keys to the transmitting-side computer 11.

[0025] Drawing 6 is the flow chart which showed processing of the 3rd calculating machine in an approach-type cryptocommunication system. 601 receives the enciphered session key 306 which is sent from the transmitting-side computer 11. The step stored in the session key storage area 212, 602 decrypts the enciphered session key 306 which started the code and the decryption program 241 corresponding to the encryption key 15 and cryptographic algorithm which are shared with the transmitting-side computer 11 stored in the key database 244, and was stored in the session key storage area 212. The step which stores the taken-out session key 17 in the session key storage area 212, 603 enciphers the session key 17 which started the code and the decryption program 241 corresponding to the encryption key 16 and cryptographic algorithm which are shared with the receiving-side computer 12 stored in the key database 244, and was stored in the session key storage area 212. The step which stores the enciphered session key 309 in the session key storage area 212, and 604 are steps which transmit the enciphered session key 309 which was created at step 603 to the receiving-side computer 12 by communication link I/O.

[0026] Drawing 7 is the flow chart which showed the processing to which the receiving-side calculating machine 12 in the cryptocommunication system of this method decrypts a message 18. The step which stores in the message storage area 213 the cipher 305 which 701 received from the transmitting-side calculating machine 11, The step which stores the enciphered session key 309 which 702 received from the 3rd computer 13 in the session key storage area 212, 703 decrypts the enciphered session key 309 which started the code and the decryption program 241 corresponding to the encryption key 16 and cryptographic algorithm which are shared with the 3rd computer stored in the key database 244, and was stored in the session key storage area 212. The step which stores the taken-out session key 17 in the session key storage area 212, and the session key 17 with which 704 took out at step 703, It is the step which decrypts the cipher 305 which started the code and the decryption program 241 corresponding to the code cipher system flag 211 for session keys, and was stored in the message storage area 213, and takes out a message 18.

[0027] Drawing 8 is drawing showing the another implementation approach of the cryptocommunication system of this method. The transmittal mode of a session key differs from drawing 1 , and the following procedure performs cryptocommunication.

[0028] (1) Ask the cryptographic algorithm method used for both cryptocommunication from the transmitting-side computer 11 to the receiving-side computer 12.

[0029] (2) The receiving-side computer 12 chooses the cryptographic algorithm method used for both cryptocommunication, and notifies it to the transmitting-side computer 11.

[0030] (3) The transmitting-side computer 11 generates the session key 17 which satisfies the requirements specified by the cryptographic algorithm notified from (a) receiving-side computer 12.

(b) Be with the session key 17 and encipher an outgoing message 18 as the cryptographic algorithm notified from the receiving-side computer 12. Furthermore, the session key 17 is enciphered with the cryptographic algorithm 1 and the encryption key 15 which are shared between the 3rd computer 13. The outgoing message and session key which were enciphered are transmitted to the receiving-side computer 12.

(4) The receiving-side computer 12 transmits the received session key to the 3rd computer 13.

[0031] (5) The 3rd computer 13 decrypts the enciphered session key 17 which was received from (a) transmitting-side computer 11 using the cryptographic algorithm 1 and the encryption key 15 which are shared between the transmitting-side computers 11.

(b) Encipher with the cryptographic algorithm 2 which is sharing the decrypted session key 17 between the receiving-side computers 12, and the encryption key 16, and transmit to the receiving-side computer 12.

[0032] (6) The receiving-side computer 12 decrypts the enciphered session key 17 which was received from the (a) 3rd computer 13 using the cryptographic algorithm 2 and the encryption key 16 which are shared between the 3rd computer.

(b) Decrypt the enciphered message which was received from the transmitting-side calculating machine 11 using the cryptographic algorithm and the session key 17 which were decided by the negotiation. By this method, the transmitting-side computer 11 does not carry out direct communication to the 3rd computer 13.

[0033] In the cryptocommunication system of this method, even when a negotiation goes wrong, furthermore drawing 9 makes cryptocommunication possible, it is an option and it performs cryptocommunication in the following procedure.

[0034] (1) Ask the cryptographic algorithm method used for both cryptocommunication from the transmitting-side computer 11 to the receiving-side computer 12.

[0035] (2) The receiving-side computer 12 chooses the cryptographic algorithm method used for both cryptocommunication, and notifies it to the transmitting-side computer 11.

[0036] (3) The transmitting-side computer 11 transmits a code message by the approach of Figs. 1 or 8, when cryptographic algorithm more nearly usable than (a) receiving-side computer 12 is notified.

(b) When notified that cryptographic algorithm more nearly usable than the receiving-side computer 12 does not exist, transmit a message via the 3rd computer 13.
[0037] Drawing 10 is drawing having shown the flow of processing with this method to the message at the time of a negotiation going wrong. First, when the cipher system negotiation processing 301 which chooses the cryptographic algorithm used for the cryptocommunication between the receiving-side computers 12 by the transmitting-side computer 11 goes wrong, The session key creation processing 1001 which creates the session key 1002 which suits the cryptographic algorithm 1 currently shared between the 3rd computer 13, The encryption processing 303 which enciphers a message 18 using cryptographic algorithm 1 and the session key 1002, and generates a cipher 1003, The session key 1002 is enciphered using cryptographic algorithm 1 and the encryption key 15, encryption processing 304 which generates the enciphered session key 1004 is performed, and the session key 1004 and cipher 305 which were enciphered are transmitted to the 3rd computer 13. By the 3rd computer 13, next, the enciphered session key 1004 which was received from the transmitting-side computer 11 The decryption processing 307 which decrypts using the cryptographic algorithm 1 and the encryption key 15 which are shared between the transmitting-side computers 11, and takes out the session key 1002, The decryption processing 1005 which decrypts a part for a code 305 using the session key 1002 decrypted by cryptographic algorithms 1 and 307, and takes out a message 18, The session key creation processing 1006 which creates the session key 1008 which suits the cryptographic algorithm 2 currently shared between the receiving-side computers 12, The encryption processing 1007 which enciphers a message 18 using cryptographic algorithm 2 and the session key 1008, and generates a cipher 1010, The session key 1008 is enciphered using cryptographic algorithm 2 and the encryption key 16, encryption processing 1009 which generates the enciphered session key 1011 is performed, and the session key 1011 and cipher 1010 which were enciphered are transmitted to the receiving-side computer 12. Furthermore, the cryptographic algorithm 2 which shares the enciphered session key 1011 which was received from the 3rd computer 13 between the receiving-side computer 12 between the 3rd computer 13, the decryption processing 310 which decrypt the session key 1008 using the encryption key 16, and the decryption processing 311 which decrypt a message 18 using the cryptographic algorithm 2 which shares the cipher 1010 received from the 3rd computer 13 between the 3rd computer 13, and the session key 1008 perform.
[0038] Drawing 11 is drawing showing another implementation method which enciphers a session key with a public key in the cryptocommunication system of this method.
[0039] For 1101, as for the private key of the 3rd computer 13, and 1103, the public key of the 3rd computer 13 and 1102 are [the public key of the receiving-side computer 12 and 1103] the private keys of the receiving-side computer 12.
[0040] By this method, the share key of a key can be delivered on a network by using the public key 1103 and private key 1103 of the receiving-side computer 12 instead of the share key 15 of drawing 1 instead of the public key 1101 of a computer 13 and a private key 1102, and the share key 16.
[0041] Drawing 12 is drawing having shown the more concrete example of the cryptocommunication system of this method. The transmitting-side computer which 1201 has the encryption key K1 of MULTI, and can use the compression algorithm by cryptographic algorithm MULTI and the Huffman method, 1202 has the encryption key K2 of MULTI, and the receiving-side computers 1 and 1203 which can use cryptographic algorithm MULTI have the encryption key K3 of DES. The transmitting-side computer which can use the compression algorithm by cryptographic algorithm DES and the Huffman method, The transmitting-side computer which 1204 has the encryption key K4 of FEAL, and can use the compression algorithm by cryptographic algorithm FEAL and the Huffman method, and 1205 The share key K1 of MULTI with the transmitting-side computer 1201, It has the share key K2 of MULTI with the receiving-side computer 1202, and the share key K3 of DES with the receiving-side computer 1203. The 3rd computer which can use cryptographic algorithm MULTI and cryptographic algorithm DES, and 1206 The share key K1 of MULTI with the transmitting-side computer 1201, As for the 3rd computer which has the share key K4 of FEAL with the receiving-side computer 1204, and can use cryptographic algorithm MULTI and cryptographic algorithm FEAL, and 1207, a message and 1208 are sessions.
[0042] The procedure at the time of the transmitting-side computer 1201 performing the receiving-side computer 1202 and cryptocommunication is shown below.
[0043] (1) MULTI and FEAL which are the code/compression algorithm which can use the transmitting-side computer 1201 from the transmitting-side computer 1201 to the receiving-side computer 1202, and Huffman — notify law.
[0044] (2) The receiving-side computer 1202 notifies MULTI which is the cipher system which can be used to a transmitting-side computer.
[0045] (3) The transmitting-side calculating machine 1201 generates the 64 bits user key used by (a) MULTI, and a 256-bit system key as a session key 1208.
(b) Encipher a message 1207 by MULTI using said user key and a system key, and transmit to the receiving-side computer 1202.
(c) Encipher the session key 1208 with the share key K1 of MULTI, and transmit to the 3rd computer 1205.
[0046] (4) The 3rd computer 1205 decrypts the enciphered session key which was received from (a) transmitting-side computer 1201 with MULTI and the share key K1.
(b) Encipher with the share key K2 of MULTI which is sharing the decrypted session key with the receiving-side computer 1202, and transmit to the receiving-side computer 1202.
[0047] (5) The receiving-side computer 1202 decrypts the enciphered session key which was received from the (a)

3rd computer 1205 with MULTI and the share key K2, and takes out the 64 bits user key and the 256-bit system key which are the session key 1208.
(b) Decrypt the enciphered message which was received from the transmitting-side calculating machine 1201 with an above-mentioned user key and an above-mentioned system key.
the code/compression algorithm which can be used here when the transmitting-side computer 1201 performs the receiving-side computer 1203 and cryptocommunication — Huffman — since it becomes law, the session key 1208 becomes data expressing the Huffman tree. Cryptocommunication can be performed even if it uses the session key with which configurations differ for every communications partner in this way in the case of this method.
[0048] Moreover, the 3rd computer 1205 uses no cryptographic algorithms of the transmitting-side computer 1201. For example, when the transmitting-side computer 1201 performs the receiving-side computer 1204 and cryptocommunication, the code/compression algorithm which can be used are set to FEAL. At this time, it has the share key K1 of MULTI with the transmitting-side computer 1201, and the share key K4 of FEAL with the receiving-side computer 1204, and if the 3rd computer 1206 which can use cryptographic algorithm MULTI and cryptographic algorithm FEAL exists, activation of this method will be attained.
[0049]
[Effect of the Invention] In the cryptocommunication system which performs a code or a compression communication link between the transmitting-side computer linked to a network, and a receiving-side computer using the code or compression algorithm chosen by the negotiation, cryptocommunication with many and unspecified partners like electronic commerce is made possible by carrying out the negotiation of the cryptographic algorithm or the compression algorithm used for encryption of a communication message between a transmitting-side computer and a receiving-side computer, and determining it. Furthermore, by transmitting the information used for encryption and compression-izing of a message or a message using a transmitting-side computer and a receiving-side computer, and the 3rd computer that can carry out cryptocommunication, respectively, both of transmitting-side computers and receiving-side computers will end, if information is shared between the 3rd computer. Thereby, in a transmitting-side computer and a receiving-side computer, the management about the share information that specifications differ, such as many share keys, can be simplified.

[Translation done.]

DESCRIPTION OF DRAWINGS

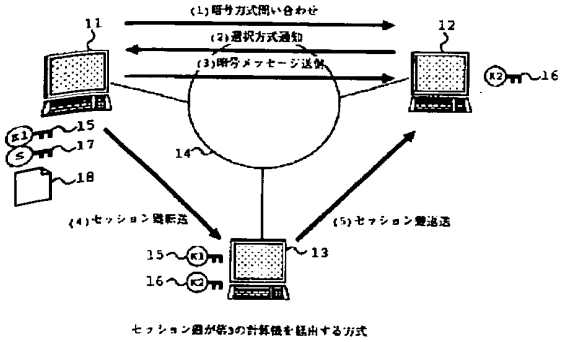
[Brief Description of the Drawings]
[Drawing 1] It is the whole block diagram showing one example of this invention.
[Drawing 2] It is drawing showing the configuration of a processor.
[Drawing 3] It is the processing flow chart of the whole which shows one example of this invention.
[Drawing 4] It is the flow chart which shows encryption processing of a transmitting-side calculating machine.
[Drawing 5] It is the flow chart which shows negotiation information creation processing of a receiving-side calculating machine.
[Drawing 6] It is the flow chart which shows session key processing of the 3rd calculating machine.
[Drawing 7] It is the flow chart which shows decryption processing of a receiving-side calculating machine.
[Drawing 8] It is the whole configuration which shows other examples of this invention.
[Drawing 9] It is the whole block diagram showing the example of further others of this invention.
[Drawing 10] It is the whole processing flow chart which shows other examples of this invention.
[Drawing 11] It is the whole block diagram showing the example of further others of this invention.
[Drawing 12] It is drawing having shown the more concrete example of a cryptocommunication system.
[Description of Notations]
11 [— Network,] — A transmitting-side computer, 12 — A receiving-side computer, 13 — The 3rd computer, 14 15 [— Message,] — An encryption key, 16 — An encryption key, 17 — A session key, 18 21 — Memory, 211 — The cipher system flag for session keys, 212 — Session key storage area, 213 — A message storage area, 214 — Program load area, 22 [— A code and a decryption program group,] — A bus, 23 — CPU, 24 — External storage, 241 242 — A session key generator, 243 — Key specification database, 244 — A key information database, 25 — Communication link I/O, the channel to a computer besides 26 —, 301 — Cipher system negotiation processing, 302 — Session key creation processing, 303 [— The enciphered session key,] — Encryption processing, 304 — Encryption processing, 305 — A cipher, 306 307 — Decryption processing, 308 — Decryption processing, 309 — The enciphered session key, 310 — Decryption processing, 311 — Decryption processing, 401 — Cryptographic algorithm listing processing, 402 — The notice processing of listing information, 403 — Cryptographic algorithm name reception, 404 — Session key creation processing, 405 — Message encryption processing, 406 — Cipher transmitting processing, 407 — Session key encryption processing, 408 — Encryption session key transmitting processing, 501 — Listing information reception, 502 — Cryptographic algorithm information comparison processing, 503 — Available cryptographic algorithm judging processing, 504 — Cryptographic algorithm name setting processing, 505 — NULL setting processing, 506 — Negotiation information transmitting processing, 601 — Session key reception, 602 — Session key decryption processing, 603 — Session key encryption processing, 604 — Session key transmitting processing, 701 — Encryption message reception, 702 — Encryption session key reception, 703 — Session key decryption processing, 704 — Message decryption processing 1001 — Session key creation processing, 1002 — A session key, 1003 — A cipher, 1004 — The enciphered session key, 1005 — Decryption processing, 1006 — Session key creation processing, 1007 — Encryption processing, 1008 — A session key, 1009 — Encryption processing, 1010 — Cipher, 1011 — The session key, 1101 which were enciphered — The public key of the 3rd computer 13, 1102 — The private key of the 3rd computer 13, 1103 — The public key of the receiving-side computer 12, 1104 [— A receiving-side computer, 1204 / — A receiving-side computer, 1205 / — The 3rd computer, 1206 / — The 3rd computer, 1207 / — A message, 1207 / — Session key] — The private key of the receiving-side computer 12, 1201 — A transmitting-side computer, 1202 — A receiving-side computer, 1203

[Translation done.]

DRAWINGS

[Drawing 1]

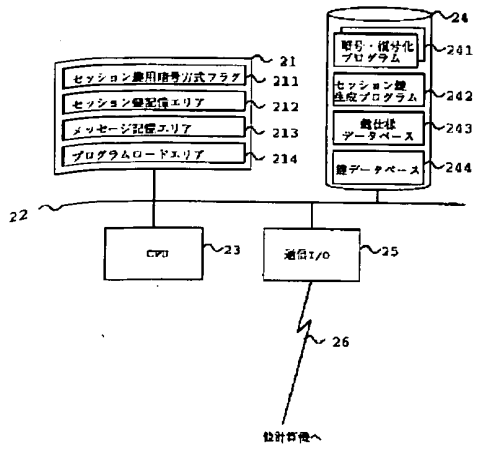
図 1



セッション鍵が第3の計算機を経由する方式

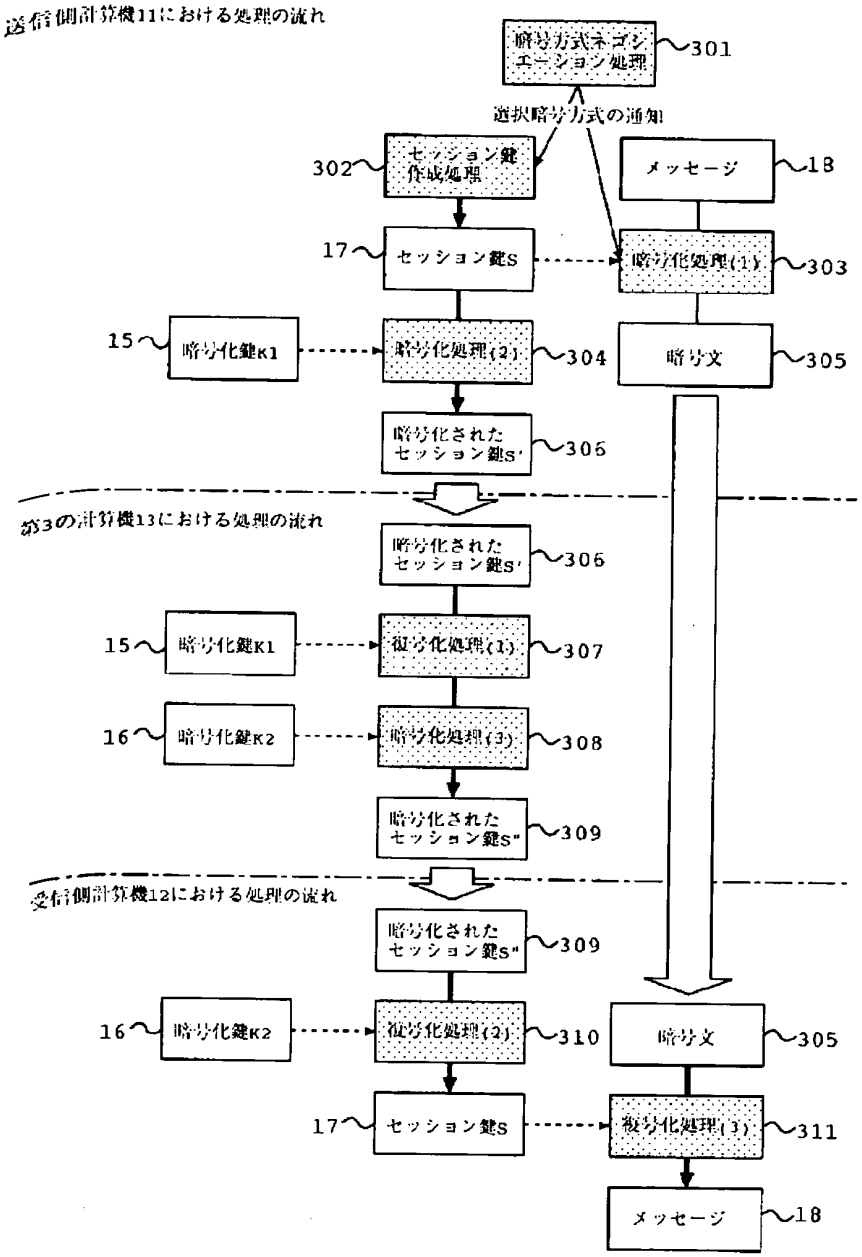
[Drawing 2]

図 2



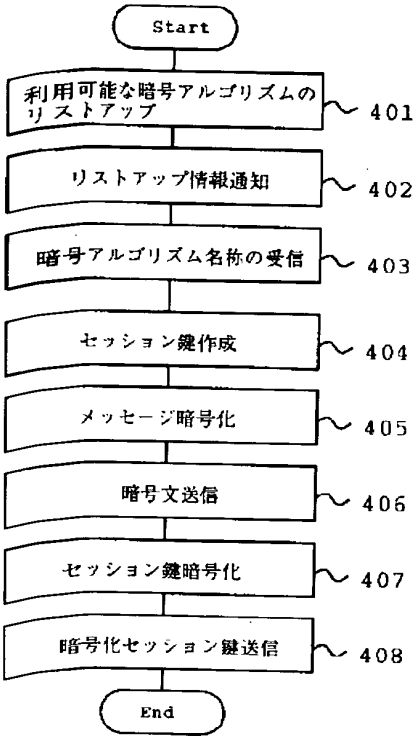
[Drawing 3]

図 3


送信側計算機11における処理の流れ
暗号方式ネゴシエーション処理
301
選択暗号方式の通知
セッション鍵作成処理
302
メッセージ
18
17
セッション鍵S
暗号化処理(1)
303
15
暗号化鍵K1
暗号化処理(2)
304
暗号文
305
暗号化されたセッション鍵S'
306
第3の計算機13における処理の流れ
暗号化されたセッション鍵S'
306
15
暗号化鍵K1
復号化処理(1)
307
16
暗号化鍵K2
暗号化処理(3)
308
暗号化されたセッション鍵S"
309
受信側計算機12における処理の流れ
暗号化されたセッション鍵S"
309
16
暗号化鍵K2
復号化処理(2)
310
暗号文
305
17
セッション鍵S
復号化処理(3)
311
メッセージ
18

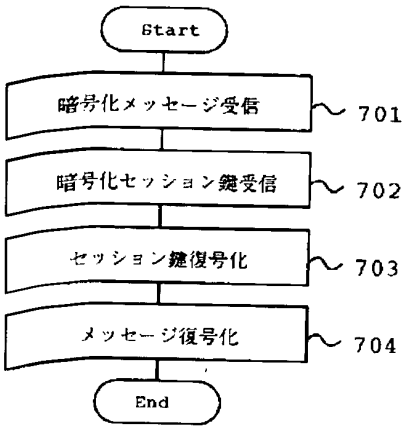
[Drawing 4]

図 4



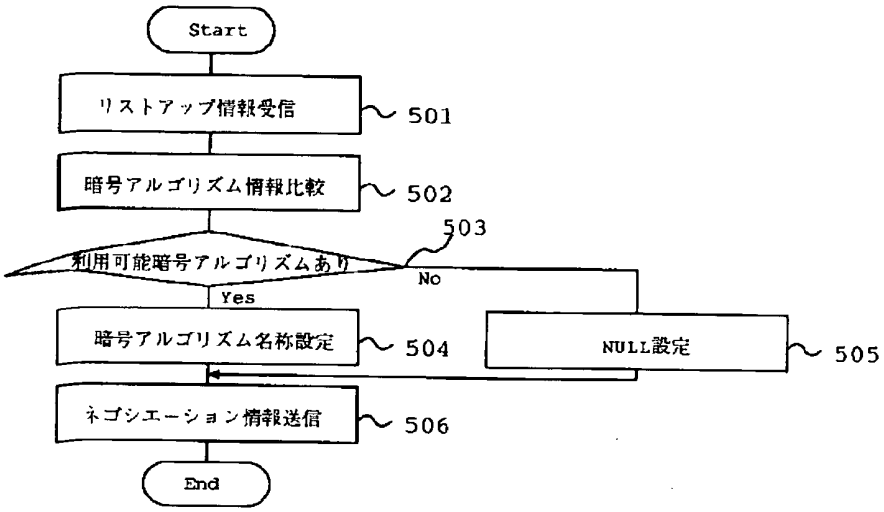
[Drawing 7]

図 7



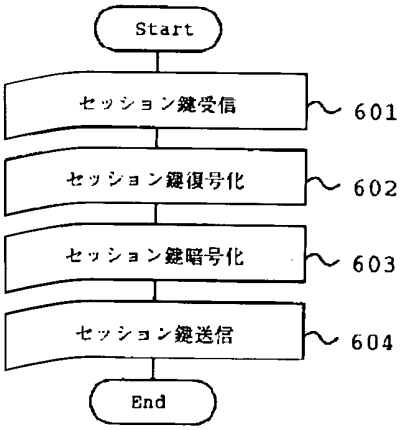
[Drawing 5]

図 5



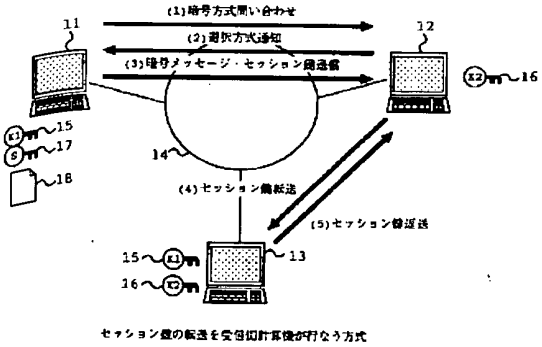
[Drawing 6]

図 6



[Drawing 8]

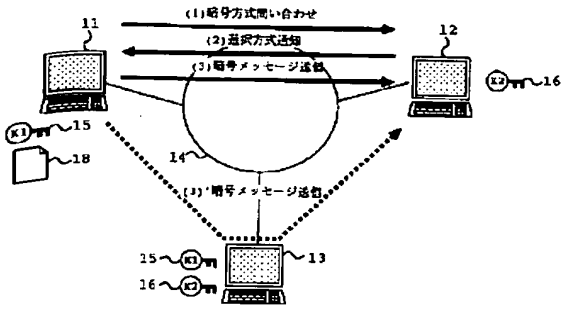
図 8



セッション鍵の転送を受信側計算機が行なう方式

[Drawing 9]

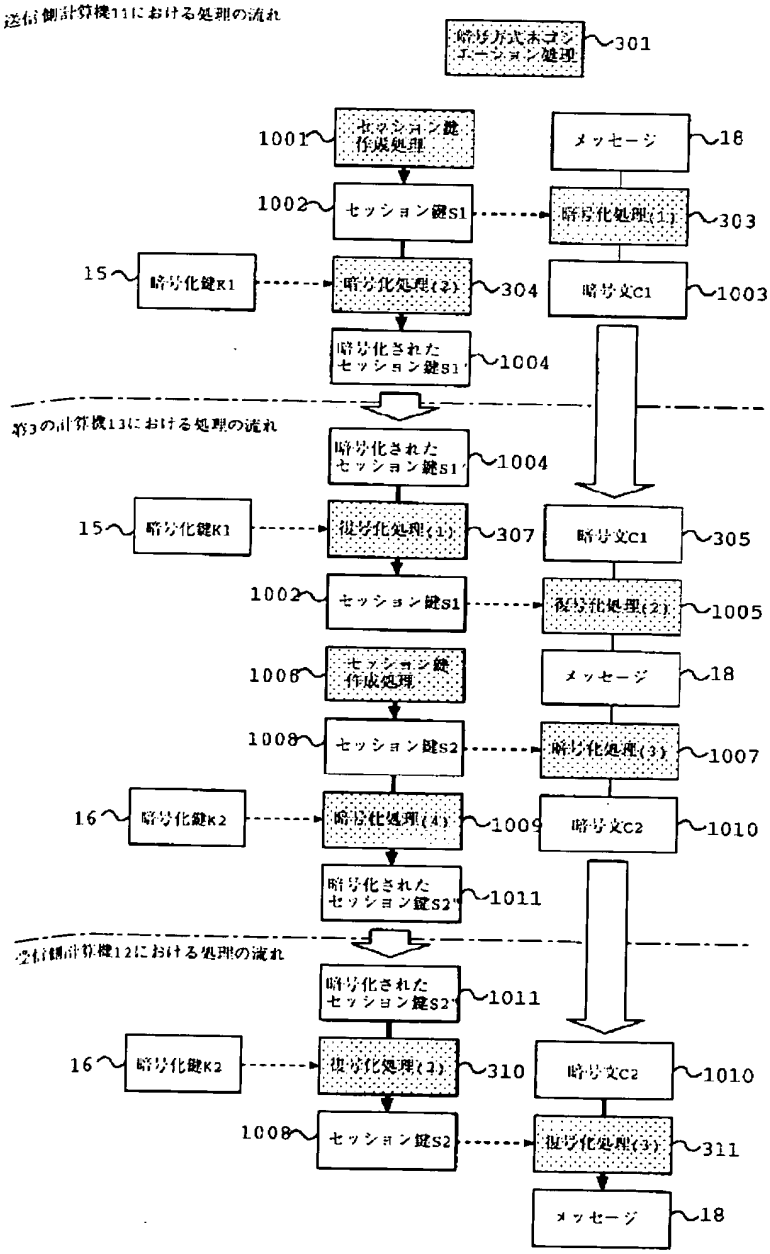
図 9



ネゴシエーションに失敗した時第3の計算機を経由する方式

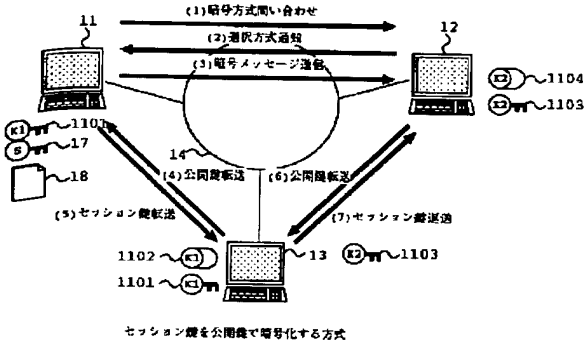
[Drawing 10]

図１０



[Drawing 11]

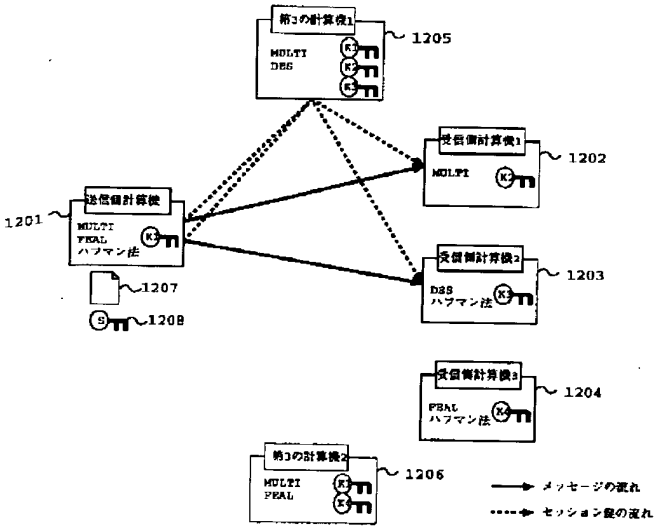
図１１



セッション鍵を公開鍵で暗号化する方式

[Drawing 12]

図１２



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－83509

(43)公開日　平成９年(1997)３月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ｚ	
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ	
	13/00	３５１			13/00	３５１Ｂ	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ	
		６５０	7259－5Ｊ			６５０Ｚ	

審査請求　未請求　請求項の数26　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平7－234998

(22)出願日　平成７年(1995)９月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　暗号通信方法および装置

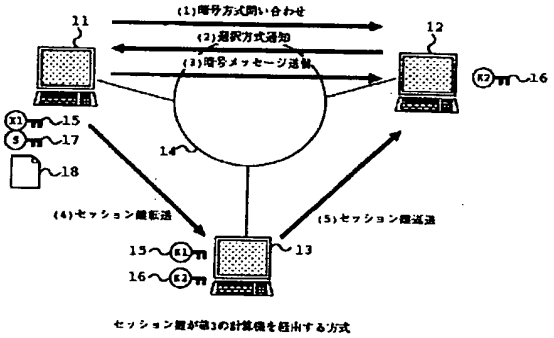
(57)【要約】　（修正有）

【課題】送信側計算機および受信側計算機の間の仕様が異なる多数の共有情報、例えば暗号鍵の管理を簡略化する。

【解決手段】送信側計算機１１と受信側計算機１２の間で通信メッセージの暗号化に使用する暗号または圧縮アルゴリズムをネゴシエーションして決定する。更に、送信側計算機および受信側計算機とそれぞれ情報を共有することにより、前記送信側計算機および前記受信側計算機とそれぞれ暗号または圧縮通信を行なうことができる第３の計算機１３をネットワーク上に配置し、通信メッセージを暗号化するためのセッション鍵は、送信側計算機と第３の計算機間の共有鍵で暗号化し、第３の計算機に送信する。第３の計算機は受けとったセッション鍵を受信側計算機との間の共有鍵で暗号化し直し、受信側計算機に送信する。

【効果】電子取引のような不特定多数の相手との暗号通信を可能にし、送受の計算機共第３の計算機間の共有鍵のみ保持すれば済むので、仕様が異なる多数の共有情報を簡略化できる。

図１



セッション鍵が第3の計算機を経由する方式

1

【特許請求の範囲】

【請求項１】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、

前記送信側計算機および前記受信側計算機とそれぞれ暗号通信することができる第３の計算機を利用して、メッセージもしくはメッセージの暗号化および圧縮化に使用する情報を送信することを特徴とする暗号通信方法。

【請求項２】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、前記送信側計算機および前記受信側計算機とそれぞれ暗号通信することができる第３の計算機をネットワーク上に配置し、メッセージの暗号化に使用する情報のうちセッション鍵を第３の計算機経由で暗号化して送信することを特徴とする請求項１記載の暗号通信方法。

【請求項３】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、受信側計算機は復号化できない暗号化が行なわれたセッション鍵を受信した場合、当該セッション鍵を第３の計算機に転送し、当該第３の計算機は当該セッション鍵を前記受信側計算機が復号化できるように処理した後、前記受信側計算機に返送することを特徴とする請求項１記載の暗号通信方法。

【請求項４】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、前記送信側計算機および前記受信側計算機とそれぞれ通信することができる第３の計算機をネットワーク上に配置し、ネゴシエーションに失敗した場合にメッセージを第３の計算機経由で暗号化して送信することを特徴とする請求項１記載の暗号通信方法。

【請求項５】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、メッセージの暗号化に使用する情報のうちセッション鍵の仕様をネゴシエーションにより決定することを特徴とする請求項１記載の暗号通信方法。

【請求項６】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、メッセージの圧縮に関する情報をネゴシエーションにより決定することを特徴とする請求項１記載の暗号通信方法。

2

【請求項７】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、セッション鍵の暗号化を、送信側計算機と第３の計算機との間で共有した慣用鍵と、受信側計算機と第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項２記載の暗号通信方法。

【請求項８】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、セッション鍵の暗号化を、送信側計算機と第３の計算機との間で共有した慣用鍵と、受信側計算機と第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項３記載の暗号通信方法。

【請求項９】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、セッション鍵の暗号化を、第３の計算機の公開鍵を送信側計算機に、受信側計算機の公開鍵を第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項２記載の暗号通信方法。

【請求項１０】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、セッション鍵の暗号化を、第３の計算機の公開鍵を送信側計算機に、受信側計算機の公開鍵を第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項３記載の暗号通信方法。

【請求項１１】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、ネゴシエーションに失敗した場合のメッセージの暗号化に送信側計算機と第３の計算機との間で共有した慣用鍵と、受信側計算機と第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項４記載の暗号通信方法。

【請求項１２】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、ネゴシエーションに失敗した場合のメッセージの暗号化に第３の計算機の公開鍵を送信側計算機に、受信側計算機の公開鍵を第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項４記載の暗号通信方法。

【請求項１３】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、送信側計算機と受信側計算機との間の経路情報を利用して、メッセージの暗号化に使用する情報のうちセッション鍵の仕様を決定することを特徴とする請求項５記載の暗号通信方法。

【請求項１４】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信装置において、
前記送信側計算機および前記受信側計算機とそれぞれ暗号通信可能な第３の計算機を備え、前記送信側計算機はメッセージもしくはメッセージの暗号化および圧縮化に使用する情報を前記第３の計算機を介して送信することを特徴とする暗号通信装置。

【請求項１５】前記送信側計算機および前記受信側計算機とそれぞれ暗号通信することができる第３の計算機をネットワーク上に配置し、メッセージの暗号化に使用する情報のうちセッション鍵を前記第３の計算機経由で暗号化して送信することを特徴とする請求項１４記載の暗号通信装置。

【請求項１６】前記受信側計算機は復号化できない暗号化が行なわれたセッション鍵を受信した場合、当該セッション鍵を前記第３の計算機に転送し、当該第３の計算機は当該セッション鍵を前記受信側計算機が復号化可能に処理した後、前記受信側計算機に返送することを特徴とする請求項１４記載の暗号通信装置。

【請求項１７】前記送信側計算機および前記受信側計算機とそれぞれ通信することができる第３の計算機をネットワーク上に配置し、前記送信側計算機は前記受信側計算機とネゴシエーションに失敗した場合、メッセージを第３の計算機経由で暗号化して送信することを特徴とする請求項１４記載の暗号通信装置。

【請求項１８】メッセージの暗号化に使用する情報のうちセッション鍵の仕様をネゴシエーションにより決定することを特徴とする請求項１４記載の暗号通信装置。

【請求項１９】メッセージの圧縮に関する情報をネゴシエーションにより決定することを特徴とする請求項１４記載の暗号通信装置。

【請求項２０】セッション鍵の暗号化を、前記送信側計算機と前記第３の計算機との間で共有した慣用鍵と、前記受信側計算機と前記第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項１５記載の暗号通信装置。

【請求項２１】セッション鍵の暗号化を、前記送信側計算機と前記第３の計算機との間で共有した慣用鍵と、前記受信側計算機と前記第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項１６記載の暗号通信装置。

【請求項２２】セッション鍵の暗号化を、前記第３の計算機の公開鍵を前記送信側計算機に、前記受信側計算機の公開鍵を前記第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項１５記載の暗号通信装置。

【請求項２３】セッション鍵の暗号化を、前記第３の計算機の公開鍵を前記送信側計算機に、前記受信側計算機の公開鍵を前記第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項１６記載の暗号通信装置。

【請求項２４】ネゴシエーションに失敗した場合のメッセージの暗号化に前記送信側計算機と前記第３の計算機との間で共有した慣用鍵と、前記受信側計算機と前記第３の計算機との間で共有した慣用鍵を用いて暗号化することを特徴とする請求項１７記載の暗号通信装置。

【請求項２５】ネゴシエーションに失敗した場合のメッセージの暗号化に前記第３の計算機の公開鍵を前記送信側計算機に、前記受信側計算機の公開鍵を前記第３の計算機にそれぞれ持たせ、前記公開鍵暗号を用いて暗号化することを特徴とする請求項１７記載の暗号通信装置。

【請求項２６】前記送信側計算機と前記受信側計算機との間の経路情報を利用して、メッセージの暗号化に使用する情報のうちセッション鍵の仕様を決定することを特徴とする請求項１８記載の暗号通信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号アルゴリズムを使用して暗号通信を行なう暗号通信方法および装置に係わり、特に複数の送信元もしくは送信先が存在する暗号通信方法および装置に関する。

【０００２】

【従来の技術】従来、複数の送信元および送信先が存在する暗号通信システムの場合、各計算機はそれぞれの送信先毎に共有鍵を管理する必要があった。この鍵管理を軽減するための方法として、ＩＳＯのドラフト（ISO/IEC DIS 11770-2 Mechanism13）で以下の方式に基づいた鍵管理方式が提案されている。

【０００３】（１）送信先および受信先と鍵を共有する鍵管理センターをネットワーク上に配置する。

【０００４】（２）メッセージはランダムに生成したセッション鍵で暗号化、セッション鍵は送信側と鍵管理センターとの間で共有している鍵で暗号化し、両者を受信側に送付する。

【０００５】（３）受信側は暗号化されたセッション鍵を鍵管理センターに送付する。

【０００６】（４）鍵管理センターはセッション鍵を復号した後、鍵管理センターと受信側との間で共有してい

る鍵で暗号化し、受信側に送付する。

【０００７】また、暗号通信に使用する暗号アルゴリズムは、複数の送信元および送信先が存在する場合、通信相手によって使用する暗号アルゴリズムを切替える必要がある。このため、ネットワークに接続した計算機同士で、暗号通信に使用する暗号アルゴリズムをネゴシエーションして選択するプログラムインタフェースとして、ＧＳＳ－ＡＰＩ（Generic Security Service Application Program Interface）でネゴシエーションメカニズムが提案されている。ＧＳＳ－ＡＰＩネゴシエーションメカニズムは、以下の処理の概要を定めたものである。

【０００８】（１）送信側がサポートしている暗号アルゴリズム種別を受信側に通知する処理。

【０００９】（２）受信側が受信した暗号アルゴリズム種別から利用可能なものを選択し、送信側に返送する処理。

【００１０】

【発明が解決しようとする課題】ネットワークを利用して商取引等を行なう際には、不正行為を防止するために通信メッセージを暗号化する必要がある。通常、メッセージの暗号化を行なう暗号アルゴリズムは標準となる方式が存在せず、各種の方式が提案されている。暗号アルゴリズムで使用する暗号化鍵は、アルゴリズムによって仕様が異なっている。例えば、ＤＥＳの場合は、暗号化鍵の鍵長が５６ビットであるのに対して、ＭＵＬＴＩを使用する場合は鍵長が３２０ビットになる。このため、複数の送信先との間で暗号通信を行なう計算機は、各送信先毎に異なった仕様の暗号鍵を保持する必要があった。

【００１１】本発明は、複数の送信先を持ち、かつ各送信先との間でネゴシエーションにより選択した暗号あるいは圧縮アルゴリズムを使用して暗号通信を行なう暗号通信システムにおいて、送信側計算機および受信側計算機の間の多数の共有情報、例えば共有鍵の管理を簡略化することを目的とする。

【００１２】

【課題を解決するための手段】上記課題を解決するために本発明では、ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて暗号通信を行なうために、送信側計算機と暗号または圧縮アルゴリズム１とその共有鍵１を共有し、かつ、受信側計算機と暗号または圧縮アルゴリズム２とその共有鍵２を共有することにより、前記送信側計算機および前記受信側計算機とそれぞれ暗号または圧縮通信を行なうことができる第３の計算機をネットワーク上に配置し、送信側計算機と受信側計算機の間でメッセージの暗号化に使用する暗号または圧縮アルゴリズムをネゴシエーションして決定する処理を行ない、送信側計算機では、ネゴシエーションした暗号または圧縮アルゴリズムに対応した付加情報を生成する処理と、メッセージをネゴシエーションした暗号または圧縮アルゴリズムと前記付加情報で暗号化または圧縮化し、暗号化メッセージを生成する処理と、前記付加情報を前記暗号アルゴリズム１および共有鍵１で暗号化し、暗号化付加情報を生成する処理と、前記暗号化メッセージを受信側計算機に送信する処理と、前記暗号化付加情報を第３の計算機に送信する処理を行ない、第３の計算機では、送信側計算機より受信した暗号化付加情報を暗号アルゴリズム１および共有鍵１で復号化し、付加情報を取り出す処理と、前記付加情報を受信側計算機と共有している暗号アルゴリズム２および共有鍵２で暗号化し、暗号化付加情報を生成する処理と、前記暗号化付加情報を受信側計算機に送信する処理を行ない、受信側計算機では、第３の計算機より受信した暗号化付加情報を暗号アルゴリズム２および共有鍵２で復号化し、付加情報を取り出す処理と、送信側計算機より受信した暗号化メッセージをネゴシエーションした暗号アルゴリズムと前記付加情報で復号化し、メッセージを取り出す処理を順に実行する。

【００１３】また、送信側計算機と受信側計算機の間での暗号または圧縮アルゴリズムのネゴシエーションが失敗した場合、送信側計算機では、第３の計算機と共有している暗号または圧縮アルゴリズム１に適用可能な付加情報を生成する処理と、メッセージを暗号アルゴリズム１および前記付加情報で暗号化または圧縮化し、暗号化メッセージを生成する処理と、前記付加情報を暗号または圧縮アルゴリズム１および共有鍵１で暗号化し、暗号化付加情報を生成する処理と、前記暗号化メッセージおよび暗号化付加情報を第３の計算機に送信する処理を行ない、第３の計算機では、送信側計算機より受信した暗号化付加情報を暗号または圧縮アルゴリズム１および共有鍵１で復号化し、付加情報を取り出す処理と、送信側計算機より受信した暗号化メッセージを暗号または圧縮アルゴリズム１および前記付加情報で復号化し、メッセージを取り出す処理と、受信側計算機と共有している暗号または圧縮アルゴリズム２に適用可能な付加情報を生成する処理と、メッセージを暗号または圧縮アルゴリズム２および前記付加情報で暗号化し、暗号化メッセージを生成する処理と、前記付加情報を暗号または圧縮アルゴリズム２および共有鍵２で暗号化し、暗号化付加情報を生成する処理と、前記暗号化メッセージおよび暗号化付加情報を受信側計算機に送信する処理を行ない、受信側計算機では、第３の計算機より受信した暗号化付加情報を暗号または圧縮アルゴリズム２および共有鍵２で復号化し、付加情報を取り出す処理と、第３の計算機より受信した暗号化メッセージを暗号または圧縮アルゴリズム２および前記付加情報で復号化し、メッセージを取り出す処理を順に実行する。

【００１４】

【作用】本発明の暗号通信システムでは、送信側計算機と受信側計算機の間でメッセージの暗号化に使用する暗号または圧縮アルゴリズムをネゴシエーションすることにより、電子取引のような不特定多数の相手との暗号通信を可能にする。更に、送信側計算機および受信側計算機と鍵を共有する第３の計算機をネットワーク上に配置し、ネゴシエーションの結果に応じて付加情報もしくはメッセージを第３の計算機経由で送信することにより、送信側計算機および受信側計算機はどちらも第３の計算機との間の共有情報のみ保持すれば暗号または圧縮通信が可能になるので、多数の共有情報、例えば共有鍵の管理を簡略化することができる。

【００１５】

【実施例】本発明の一実施例を、図１から図７を用いて説明する。図１は、本方式の暗号通信システムの概要を示す図である。１１は送信側計算機、１２は受信側計算機、１３は送信側計算機１１および、受信側計算機１２と通信を行なうことのできる第３の計算機、１４は送信側計算機１１、受信側計算機１２、第３の計算機１３との間のネットワーク、１５は送信側計算機１１と第３の計算機１３との間で共有している暗号アルゴリズム１に適用可能な暗号化鍵、１６は受信側計算機１２と第３の計算機１３との間で共有している暗号アルゴリズム２に適用可能な暗号化鍵、１７は送信側計算機１１でランダムに生成するセッション鍵、１８は送信側計算機１１より受信側計算機１２に送信するメッセージである。本システムでは、以下の手続きにより送信側計算機１１と受信側計算機１２の間の暗号通信を行なう。

【００１６】（１）送信側計算機１１から受信側計算機１２に対して、両者の暗号通信に使用する暗号アルゴリズム方式の問い合わせを行なう。

【００１７】（２）受信側計算機１２は、両者の暗号通信に使用する暗号アルゴリズム方式を選択し、送信側計算機１１に対して通知する。

【００１８】（３）送信側計算機１１は、

（ａ）受信側計算機１２より通知された暗号アルゴリズムが指定する要件を満たすセッション鍵１７を生成する。

（ｂ）受信側計算機１２より通知された暗号アルゴリズムと、セッション鍵１７を持ちいて送信メッセージ１８を暗号化し、受信側計算機１２に送信する。

（ｃ）セッション鍵１７を第３の計算機１３との間で共有している暗号アルゴリズム１と暗号化鍵１５で暗号化し、第３の計算機１３に送信する。

【００１９】（４）第３の計算機１３は、

（ａ）送信側計算機１１より受けとった暗号化されたセッション鍵１７を、送信側計算機１１との間で共有している暗号アルゴリズム１と暗号化鍵１５を用いて復号化する。

（ｂ）復号化したセッション鍵１７を受信側計算機１２との間で共有している暗号アルゴリズム２と暗号化鍵１６で暗号化し、受信側計算機１２に送信する。

【００２０】（５）受信側計算機１２は、

（ａ）第３の計算機１３より受けとった暗号化されたセッション鍵１７を第３の計算機との間で共有している暗号アルゴリズム２と暗号化鍵１６を用いて復号化する。

（ｂ）送信側計算機１１より受けとった暗号化されたメッセージをネゴシエーションで決った暗号アルゴリズムとセッション鍵１７を用いて復号化する。

ここで、送信側計算機１１と受信側計算機１２がハフマン法による圧縮アルゴリズムをサポートしている場合、メッセージをハフマン法により圧縮し、メッセージ中の伝送符号に対するハフマン木をセッション鍵として利用することもできる。

【００２１】図２は、本方式で使用する計算機の内部構成を示した図である。２１はメモリ、２１１はセッション鍵生成に使用する暗号方式のフラグ、２１２はデータ暗号化鍵記憶エリア、２１３はセッション鍵記憶エリア、２１４はメッセージ記憶エリア、２１５は各種の暗号アルゴリズムに対応した暗号・復号化プログラムをロードするエリア、２２はバス、２３はＣＰＵ、２４は外部記憶装置で、２４１は本計算機が使用できる暗号・復号化プログラム群、２４２はセッション鍵生成プログラム、２４３は暗号・復号化プログラム群２４１で使用する鍵の仕様に関するデータベース、２４４は他計算機との間で共有している鍵および、その鍵で使用する暗号アルゴリズム名称のデータベース、２５は通信Ｉ／Ｏ、２６は他計算機への通信路である。

【００２２】図３は、ネゴシエーションが成功した際のメッセージに対する本方式での処理の流れを示した図である。まず、送信側計算機１１では、受信側計算機１２との間の暗号通信に使用する暗号アルゴリズムを選択する暗号方式ネゴシエーション処理３０１に成功した場合、３０１で決定した暗号アルゴリズムに適したセッション鍵１７を作成するセッション鍵作成処理３０２と、３０１で決定した暗号アルゴリズムとセッション鍵１７を用いてメッセージ１８を暗号化し、暗号文３０５を生成する暗号化処理３０３と、第３の計算機１３との間であらかじめ決めておいた暗号アルゴリズムと暗号化鍵１５を用いてセッション鍵１７を暗号化し、暗号化されたセッション鍵３０６を生成する暗号化処理３０４を実行し、暗号化されたセッション鍵３０６を第３の計算機１３に、暗号文３０５を受信側計算機１２にそれぞれ送信する。次に第３の計算機１３では、送信側計算機１１より受けとった暗号化されたセッション鍵３０６を、送信側計算機１１との間であらかじめ決めておいた暗号アルゴリズムと暗号化鍵１５を用いて復号化する復号化処理３０７と、３０７で復号化したセッション鍵を、受信側計算機１２との間であらかじめ決めておいた暗号アルゴリズムと暗号化鍵１６を用いて暗号化し、暗号化された

セッション鍵３０９を生成する暗号化処理３０８を実行し、暗号化されたセッション鍵３０９を受信側計算機１２に送信する。更に受信側計算機１２では、第３の計算機１３より受けとった暗号化されたセッション鍵３０９を、第３の計算機１３との間であらかじめ決めておいた暗号アルゴリズムと暗号化鍵１６を用いてセッション鍵１７を復号化する復号化処理３１０と、送信側計算機１１より受けとった暗号文３０５を、３０１で決定した暗号アルゴリズムとセッション鍵１７を用いてメッセージ１８を復号化する復号化処理３１１を実行する。

【００２３】図４は、本方式の暗号通信システムにおける送信側計算機１１の処理を示したフローチャートである。４０１は暗号・復号化プログラム群２４１をサーチして送信側計算機１１の使用可能な暗号アルゴリズムをリストアップする処理を行なうステップ、４０２はステップ４０１でリストアップした暗号アルゴリズム名称を受信側計算機１２に通知するステップ、４０３は受信計算機１２が選択した暗号アルゴリズム名称を受信し、セッション鍵用暗号方式フラグ２１１に設定するステップ、４０４はセッション鍵用暗号方式フラグ２１１に適切な暗号方式が格納されている場合、セッション鍵生成プログラム２４２を起動し、鍵仕様データベース２４３に基づきセッション鍵１７を作成し、セッション鍵記憶エリア２１２に格納するステップ、４０５はステップ４０５で作成したセッション鍵１７と、セッション鍵用暗号方式フラグ２１１に対応する暗号・復号化プログラム２４１を起動してメッセージ１８を暗号化し、暗号文３０５を生成するステップ、４０６はステップ４０５で作成した暗号文３０５を通信Ｉ／Ｏ２５により受信側計算機１２に送信するステップ、４０７は鍵データベース２４４中に格納した第３の計算機１３との共有暗号化鍵１５および、暗号アルゴリズムに対応する暗号・復号化プログラム２４１を起動してセッション鍵記憶エリア２１２に格納したセッション鍵１７を暗号化し、暗号化されたセッション鍵３０６をセッション鍵記憶エリア２１２に格納するステップ、４０８はステップ４０７で作成した暗号化されたセッション鍵３０６を通信Ｉ／Ｏ２５により第３の計算機１３に送信するステップである。

【００２４】図５は、本方式の暗号通信システムにおける受信側計算機１２がセッション鍵１７作成に使用する暗号アルゴリズムを選択する処理を示したフローチャートである。５０１は送信側計算機１１より送られてくる暗号アルゴリズム名称リストを受信するステップ、５０２はステップ５０１で受信した暗号アルゴリズム名称リストと、受信側計算機１２の暗号・復号化プログラム群２４１を比較するステップ、５０３はセッション鍵用暗号方式フラグ２１１に利用可能な暗号アルゴリズムが設定されているか判定するステップ、５０４はセッション鍵用暗号方式フラグ２１１に両者に共通する暗号アルゴリズムの名称を設定するステップ、５０５はセッション鍵用暗号方式フラグ２１１にＮＵＬＬを設定するステップ、５０６はセッション鍵用暗号方式フラグ２１１の内容を送信側計算機１１に送信するステップである。

【００２５】図６は、方法式の暗号通信システムにおける第３の計算機の処理を示したフローチャートである。６０１は送信側計算機１１より送られてくる暗号化されたセッション鍵３０６を受信し、セッション鍵記憶エリア２１２に格納するステップ、６０２は鍵データベース２４４中に格納した送信側計算機１１と共有している暗号化鍵１５および暗号アルゴリズムに対応する暗号・復号化プログラム２４１を起動してセッション鍵記憶エリア２１２に格納した暗号化されたセッション鍵３０６を復号化し、取り出したセッション鍵１７をセッション鍵記憶エリア２１２に格納するステップ、６０３は鍵データベース２４４中に格納した受信側計算機１２と共有している暗号化鍵１６および暗号アルゴリズムに対応する暗号・復号化プログラム２４１を起動してセッション鍵記憶エリア２１２に格納したセッション鍵１７を暗号化し、暗号化されたセッション鍵３０９をセッション鍵記憶エリア２１２に格納するステップ、６０４はステップ６０３で作成した暗号化されたセッション鍵３０９を通信Ｉ／Ｏにより受信側計算機１２に送信するステップである。

【００２６】図７は、本方式の暗号通信システムにおける受信側計算機１２がメッセージ１８を復号化する処理を示したフローチャートである。７０１は送信側計算機１１より受信した暗号文３０５をメッセージ記憶エリア２１３に格納するステップ、７０２は第３の計算機１３より受信した暗号化されたセッション鍵３０９をセッション鍵記憶エリア２１２に格納するステップ、７０３は鍵データベース２４４中に格納した第３の計算機と共有している暗号化鍵１６および暗号アルゴリズムに対応する暗号・復号化プログラム２４１を起動してセッション鍵記憶エリア２１２に格納した暗号化されたセッション鍵３０９を復号化し、取り出したセッション鍵１７をセッション鍵記憶エリア２１２に格納するステップ、７０４はステップ７０３で取り出したセッション鍵１７と、セッション鍵用暗号暗号方式フラグ２１１に対応する暗号・復号化プログラム２４１を起動してメッセージ記憶エリア２１３に格納された暗号文３０５を復号化し、メッセージ１８を取り出すステップである。

【００２７】図８は本方式の暗号通信システムの別の実現方法を示す図である。図１とはセッション鍵の転送方式が異なっており、以下の手続きにより暗号通信を行なう。

【００２８】（１）送信側計算機１１から受信側計算機１２に対して、両者の暗号通信に使用する暗号アルゴリズム方式の問い合わせを行なう。

【００２９】（２）受信側計算機１２は、両者の暗号通信に使用する暗号アルゴリズム方式を選択し、送信側計

算機１１に対して通知する。

【００３０】（３）送信側計算機１１は、

（ａ）受信側計算機１２より通知された暗号アルゴリズムが指定する要件を満たすセッション鍵１７を生成する。

（ｂ）受信側計算機１２より通知された暗号アルゴリズムと、セッション鍵１７を持ちいて送信メッセージ１８を暗号化する。更にセッション鍵１７を第３の計算機１３との間で共有している暗号アルゴリズム１と暗号化鍵１５で暗号化する。暗号化した送信メッセージおよびセッション鍵は受信側計算機１２に送信する。

（４）受信側計算機１２は、受けとったセッション鍵を第３の計算機１３に転送する。

【００３１】（５）第３の計算機１３は、

（ａ）送信側計算機１１より受けとった暗号化されたセッション鍵１７を、送信側計算機１１との間で共有している暗号アルゴリズム１と暗号化鍵１５を用いて復号化する。

（ｂ）復号化したセッション鍵１７を受信側計算機１２との間で共有している暗号アルゴリズム２と暗号化鍵１６で暗号化し、受信側計算機１２に送信する。

【００３２】（６）受信側計算機１２は、

（ａ）第３の計算機１３より受けとった暗号化されたセッション鍵１７を第３の計算機との間で共有している暗号アルゴリズム２と暗号化鍵１６を用いて復号化する。

（ｂ）送信側計算機１１より受けとった暗号化されたメッセージをネゴシエーションで決った暗号アルゴリズムとセッション鍵１７を用いて復号化する。本方式では、送信側計算機１１は第３の計算機１３に直接通信できなくてもよい。

【００３３】図９は本方式の暗号通信システムにおいて、ネゴシエーションが失敗した場合でも暗号通信を可能にする更に別の方法で、以下の手続きにより暗号通信を行なう。

【００３４】（１）送信側計算機１１から受信側計算機１２に対して、両者の暗号通信に使用する暗号アルゴリズム方式の問い合わせを行なう。

【００３５】（２）受信側計算機１２は、両者の暗号通信に使用する暗号アルゴリズム方式を選択し、送信側計算機１１に対して通知する。

【００３６】（３）送信側計算機１１は、

（ａ）受信側計算機１２より使用可能な暗号アルゴリズムが通知された場合は第１図もしくは第８図の方法により暗号メッセージを送信する。

（ｂ）受信側計算機１２より使用可能な暗号アルゴリズムが存在しないと通知された場合は、第３の計算機１３を経由してメッセージを送信する。

【００３７】図１０は、ネゴシエーションが失敗した際のメッセージに対する本方式での処理の流れを示した図である。まず、送信側計算機１１では、受信側計算機１２との間の暗号通信に使用する暗号アルゴリズムを選択する暗号方式ネゴシエーション処理３０１に失敗した場合、第３の計算機１３との間で共有している暗号アルゴリズム１に適合するセッション鍵１００２を作成するセッション鍵作成処理１００１と、暗号アルゴリズム１とセッション鍵１００２を用いてメッセージ１８を暗号化し、暗号文１００３を生成する暗号化処理３０３と、暗号アルゴリズム１と暗号化鍵１５を用いてセッション鍵１００２を暗号化し、暗号化されたセッション鍵１００４を生成する暗号化処理３０４を実行し、暗号化されたセッション鍵１００４と暗号文３０５を第３の計算機１３に送信する。次に第３の計算機１３では、送信側計算機１１より受けとった暗号化されたセッション鍵１００４を、送信側計算機１１との間で共有する暗号アルゴリズム１と暗号化鍵１５を用いて復号化し、セッション鍵１００２を取り出す復号化処理３０７と、暗号分３０５を暗号アルゴリズム１と３０７で復号化したセッション鍵１００２を用いて復号化し、メッセージ１８を取り出す復号化処理１００５と、受信側計算機１２との間で共有している暗号アルゴリズム２に適合するセッション鍵１００８を作成するセッション鍵作成処理１００６と、暗号アルゴリズム２とセッション鍵１００８を用いてメッセージ１８を暗号化し、暗号文１０１０を生成する暗号化処理１００７と、暗号アルゴリズム２と暗号化鍵１６を用いてセッション鍵１００８を暗号化し、暗号化されたセッション鍵１０１１を生成する暗号化処理１００９を実行し、暗号化されたセッション鍵１０１１と暗号文１０１０を受信側計算機１２に送信する。更に受信側計算機１２では、第３の計算機１３より受けとった暗号化されたセッション鍵１０１１を、第３の計算機１３との間で共有する暗号アルゴリズム２と暗号化鍵１６を用いてセッション鍵１００８を復号化する復号化処理３１０と、第３の計算機１３より受けとった暗号文１０１０を、第３の計算機１３との間で共有する暗号アルゴリズム２とセッション鍵１００８を用いてメッセージ１８を復号化する復号化処理３１１を実行する。

【００３８】図１１は本方式の暗号通信システムにおいて、セッション鍵の暗号化を公開鍵で行なう別の実現方式を示す図である。

【００３９】１１０１は第３の計算機１３の公開鍵、１１０２は第３の計算機１３の秘密鍵、１１０３は受信側計算機１２の公開鍵、１１０３は受信側計算機１２の秘密鍵である。

【００４０】本方式では図１の共有鍵１５の代わりに計算機１３の公開鍵１１０１および秘密鍵１１０２、共有鍵１６の代わりに受信側計算機１２の公開鍵１１０３および秘密鍵１１０３を使用することにより、ネットワーク上で鍵の共有鍵の配送を行なうことができる。

【００４１】図１２は本方式の暗号通信システムのより具体的な例を示した図である。１２０１はＭＵＬＴＩの

暗号化鍵Ｋ１を持ち、暗号アルゴリズムＭＵＬＴＩおよびハフマン法による圧縮アルゴリズムを利用できる送信側計算機、１２０２はＭＵＬＴＩの暗号化鍵Ｋ２を持ち、暗号アルゴリズムＭＵＬＴＩを利用できる受信側計算機１、１２０３はＤＥＳの暗号化鍵Ｋ３を持ち、暗号アルゴリズムＤＥＳおよびハフマン法による圧縮アルゴリズムを利用できる送信側計算機、１２０４はＦＥＡＬの暗号化鍵Ｋ４を持ち、暗号アルゴリズムＦＥＡＬおよびハフマン法による圧縮アルゴリズムを利用できる送信側計算機、１２０５は送信側計算機１２０１とのＭＵＬＴＩの共有鍵Ｋ１と、受信側計算機１２０２とのＭＵＬＴＩの共有鍵Ｋ２と、受信側計算機１２０３とのＤＥＳの共有鍵Ｋ３を持ち、暗号アルゴリズムＭＵＬＴＩおよび暗号アルゴリズムＤＥＳを利用できる第３の計算機、１２０６は送信側計算機１２０１とのＭＵＬＴＩの共有鍵Ｋ１と、受信側計算機１２０４とのＦＥＡＬの共有鍵Ｋ４を持ち、暗号アルゴリズムＭＵＬＴＩおよび暗号アルゴリズムＦＥＡＬを利用できる第３の計算機、１２０７はメッセージ、１２０８はセッションである。

【００４２】送信側計算機１２０１が受信側計算機１２０２と暗号通信を行なう際の手続きを以下に示す。

【００４３】（１）送信側計算機１２０１から受信側計算機１２０２に対して、送信側計算機１２０１が使用できる暗号／圧縮アルゴリズムであるＭＵＬＴＩ，ＦＥＡＬ，ハフマン法を通知する。

【００４４】（２）受信側計算機１２０２は、利用できる暗号方式であるＭＵＬＴＩを送信側計算機に通知する。

【００４５】（３）送信側計算機１２０１は、

（ａ）ＭＵＬＴＩで使用する６４ビットのユーザ鍵および、２５６ビットのシステム鍵をセッション鍵１２０８として生成する。

（ｂ）前記ユーザ鍵および、システム鍵を用いてメッセージ１２０７をＭＵＬＴＩで暗号化し、受信側計算機１２０２に送信する。

（ｃ）セッション鍵１２０８をＭＵＬＴＩの共有鍵Ｋ１で暗号化し、第３の計算機１２０５に送信する。

【００４６】（４）第３の計算機１２０５は、

（ａ）送信側計算機１２０１から受けとった暗号化されたセッション鍵をＭＵＬＴＩおよび共有鍵Ｋ１で復号化する。

（ｂ）復号化したセッション鍵を受信側計算機１２０２と共有しているＭＵＬＴＩの共有鍵Ｋ２で暗号化し、受信側計算機１２０２に送信する。

【００４７】（５）受信側計算機１２０２は、

（ａ）第３の計算機１２０５より受けとった暗号化されたセッション鍵をＭＵＬＴＩおよび共有鍵Ｋ２で復号化し、セッション鍵１２０８である６４ビットのユーザ鍵と２５６ビットのシステム鍵を取り出す。

（ｂ）送信側計算機１２０１より受けとった暗号化されたメッセージを上記のユーザ鍵とシステム鍵により復号化する。

ここで、送信側計算機１２０１が受信側計算機１２０３と暗号通信を行なう場合は、利用できる暗号／圧縮アルゴリズムがハフマン法になるため、セッション鍵１２０８はハフマン木を表現するデータになる。本方式の場合には、このように通信相手毎に形状の異なるセッション鍵を用いても暗号通信を行なうことができるようになる。

【００４８】また、第３の計算機１２０５は、送信側計算機１２０１の全ての暗号アルゴリズムを利用できなくてもかまわない。例えば、送信側計算機１２０１が受信側計算機１２０４と暗号通信を行なう場合、利用できる暗号／圧縮アルゴリズムはＦＥＡＬになる。この時、送信側計算機１２０１とのＭＵＬＴＩの共有鍵Ｋ１と、受信側計算機１２０４とのＦＥＡＬの共有鍵Ｋ４を持ち、暗号アルゴリズムＭＵＬＴＩおよび暗号アルゴリズムＦＥＡＬを利用できる第３の計算機１２０６が存在すれば本方式は実行可能になる。

【００４９】

【発明の効果】ネットワークに接続した送信側計算機と受信側計算機の間で、ネゴシエーションにより選択した暗号または圧縮アルゴリズムを使用して暗号または圧縮通信を行なう暗号通信システムにおいて、送信側計算機と受信側計算機の間で通信メッセージの暗号化に使用する暗号アルゴリズムまたは圧縮アルゴリズムをネゴシエーションして決定することにより、電子取引のような不特定多数の相手との暗号通信を可能にする。更に、送信側計算機および受信側計算機とそれぞれ暗号通信することができる第３の計算機を利用して、メッセージもしくはメッセージの暗号化および圧縮化に使用する情報を送信することにより、送信側計算機および受信側計算機はどちらも第３の計算機との間で情報を共有すれば済む。これにより、送信側計算機および受信側計算機において、仕様が異なる多数の共有鍵等の共有情報に関する管理を簡略化することができる。

【図面の簡単な説明】

【図１】本発明の一実施例を示す全体構成図である。

【図２】処理装置の構成を示す図である。

【図３】本発明の一実施例を示す全体の処理フローチャートである。

【図４】送信側計算機の暗号化処理を示すフローチャートである。

【図５】受信側計算機のネゴシエーション情報作成処理を示すフローチャートである。

【図６】第３の計算機のセッション鍵処理を示すフローチャートである。

【図７】受信側計算機の復号化処理を示すフローチャートである。

【図８】本発明の他の実施例を示す全体構成である。

15

【図９】本発明の更に他の実施例を示す全体構成図である。

【図１０】本発明の他の実施例を示す全体処理フローチャートである。

【図１１】本発明の更に他の実施例を示す全体構成図である。

【図１２】暗号通信システムのより具体的な例を示した図である。

【符号の説明】

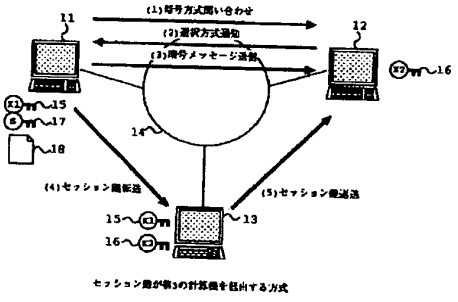
１１…送信側計算機、１２…受信側計算機、１３…第３の計算機、１４…ネットワーク、１５…暗号化鍵、１６…暗号化鍵、１７…セッション鍵、１８…メッセージ、２１…メモリ、２１１…セッション鍵用暗号方式フラグ、２１２…セッション鍵記憶エリア、２１３…メッセージ記憶エリア、２１４…プログラムロードエリア、２２…バス、２３…ＣＰＵ、２４…外部記憶装置、２４１…暗号・復号化プログラム群、２４２…セッション鍵生成プログラム、２４３…鍵仕様データベース、２４４…鍵情報データベース、２５…通信Ｉ／Ｏ、２６…他計算機への通信路、３０１…暗号方式ネゴシエーション処理、３０２…セッション鍵作成処理、３０３…暗号化処理、３０４…暗号化処理、３０５…暗号文、３０６…暗号化されたセッション鍵、３０７…復号化処理、３０８…復号化処理、３０９…暗号化されたセッション鍵、３１０…復号化処理、３１１…復号化処理、４０１…暗号アルゴリズムリストアップ処理、４０２…リストアップ＊

16

＊情報通知処理、４０３…暗号アルゴリズム名称受信処理、４０４…セッション鍵作成処理、４０５…メッセージ暗号化処理、４０６…暗号文送信処理、４０７…セッション鍵暗号化処理、４０８…暗号化セッション鍵送信処理、５０１…リストアップ情報受信処理、５０２…暗号アルゴリズム情報比較処理、５０３…利用可能暗号アルゴリズム判定処理、５０４…暗号アルゴリズム名称設定処理、５０５…ＮＵＬＬ設定処理、５０６…ネゴシエーション情報送信処理、６０１…セッション鍵受信処理、６０２…セッション鍵復号化処理、６０３…セッション鍵暗号化処理、６０４…セッション鍵送信処理、７０１…暗号化メッセージ受信処理、７０２…暗号化セッション鍵受信処理、７０３…セッション鍵復号化処理、７０４…メッセージ復号化処理１００１…セッション鍵作成処理、１００２…セッション鍵、１００３…暗号文、１００４…暗号化されたセッション鍵、１００５…復号化処理、１００６…セッション鍵作成処理、１００７…暗号化処理、１００８…セッション鍵、１００９…暗号化処理、１０１０…暗号文、１０１１…暗号化されたセッション鍵、１１０１…第３の計算機１３の公開鍵、１１０２…第３の計算機１３の秘密鍵、１１０３…受信側計算機１２の公開鍵、１１０４…受信側計算機１２の秘密鍵、１２０１…送信側計算機、１２０２…受信側計算機、１２０３…受信側計算機、１２０４…受信側計算機、１２０５…第３の計算機、１２０６…第３の計算機、１２０７…メッセージ、１２０７…セッション鍵

【図１】

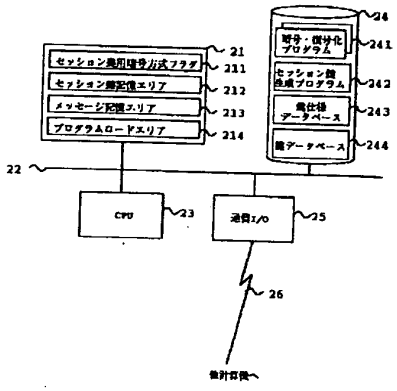
図１



セッション鍵が第３の計算機を経由する方式

【図２】

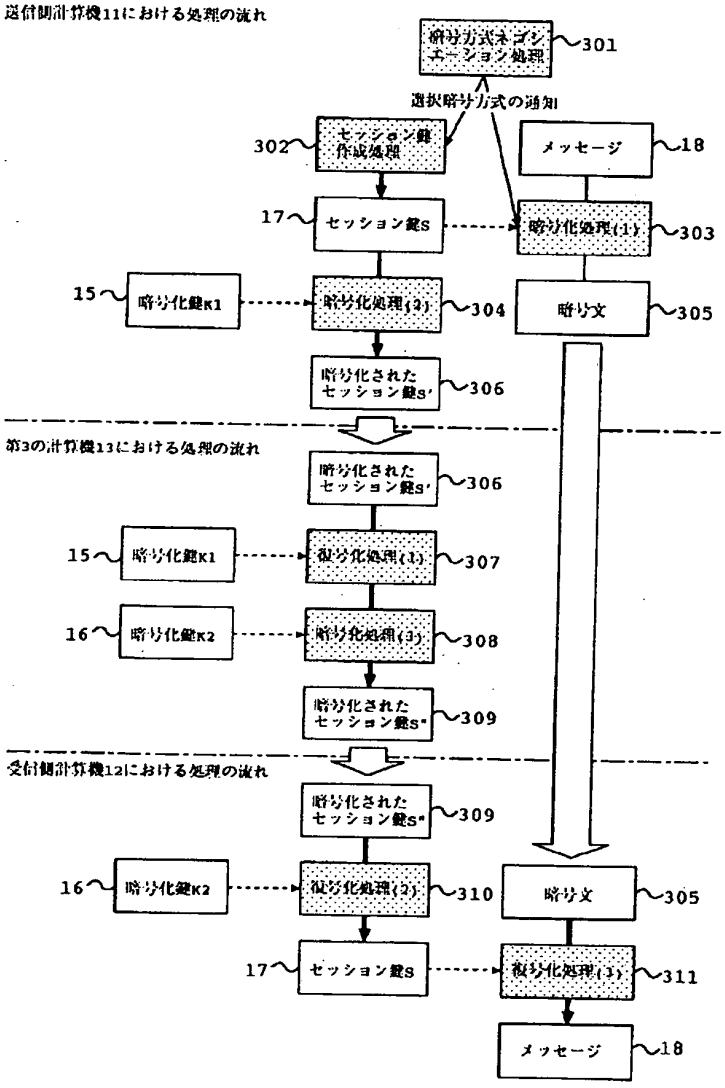
図２



009.gif

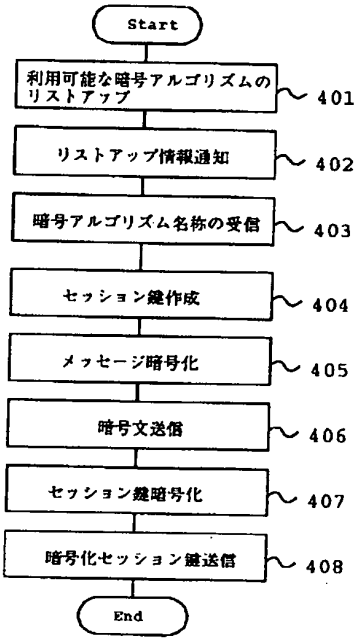
【図３】

図３



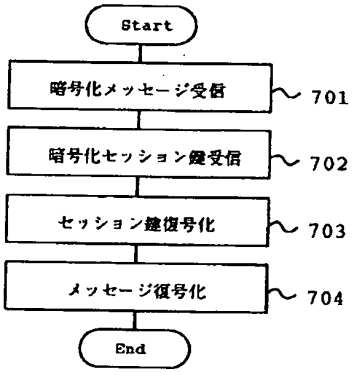
【図４】

図４



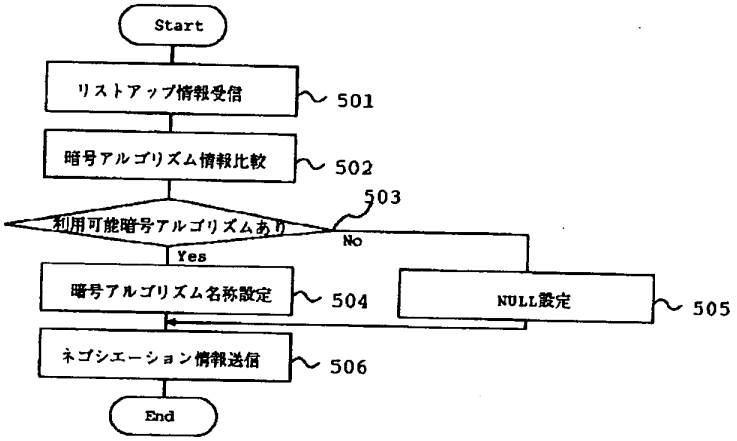
【図７】

図７



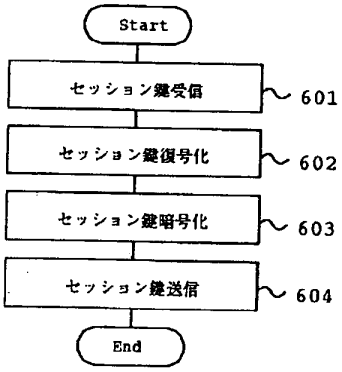
【図5】

図5



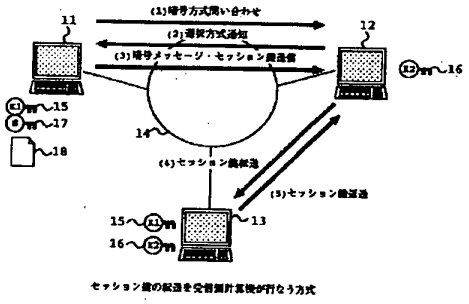
【図6】

図6



【図8】

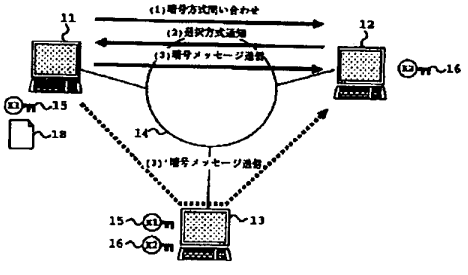
図8



セッション鍵の転送を受信端末装置が行なう方式

【図9】

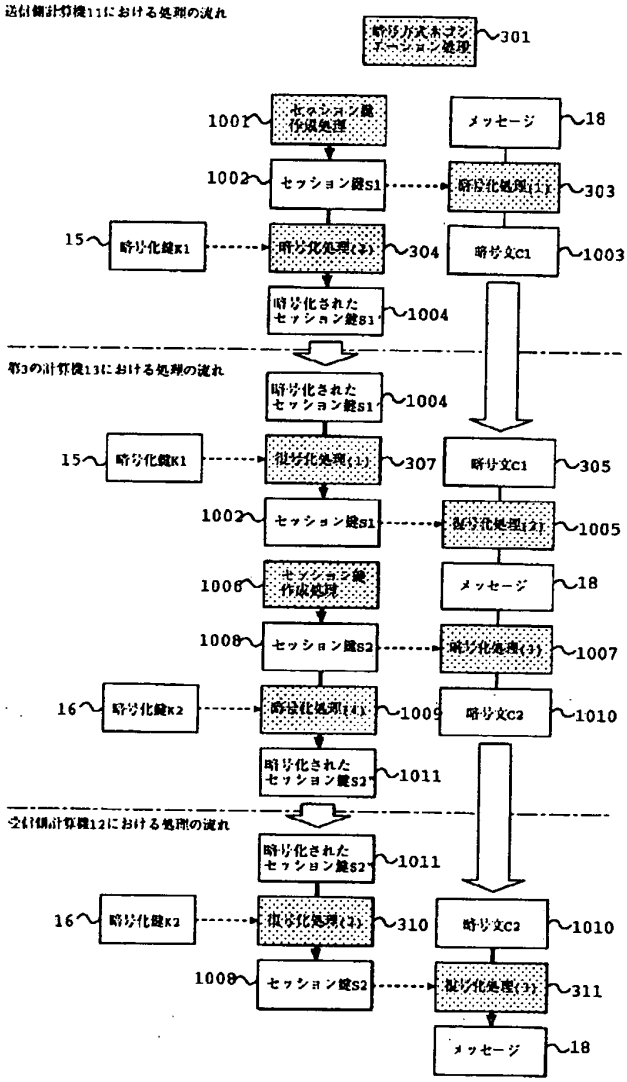
図9



ネゴシエーションに失敗した時第3の計算機を経由する方式

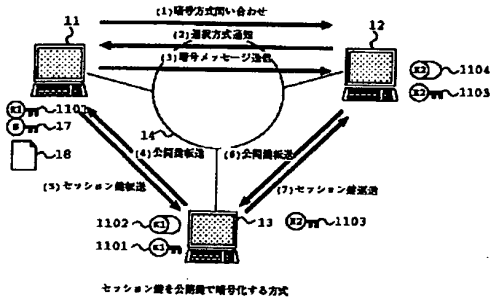
【図１０】

図１０


送信側計算機11における処理の流れ
暗号方式ネゴシエーション処理
301
セッション鍵作成処理
1001
メッセージ
18
セッション鍵S1
1002
暗号化処理(1)
303
暗号化鍵K1
15
暗号化処理(2)
304
暗号文C1
1003
暗号化されたセッション鍵S1
1004
第3の計算機13における処理の流れ
暗号化されたセッション鍵S1
1004
暗号化鍵K1
15
復号化処理(1)
307
暗号文C1
305
セッション鍵S1
1002
復号化処理(2)
1005
セッション鍵作成処理
1006
メッセージ
18
セッション鍵S2
1008
暗号化処理(3)
1007
暗号化鍵K2
16
暗号化処理(4)
1009
暗号文C2
1010
暗号化されたセッション鍵S2
1011
受信側計算機12における処理の流れ
暗号化されたセッション鍵S2
1011
暗号化鍵K2
16
復号化処理(1)
310
暗号文C2
1010
セッション鍵S2
1008
復号化処理(2)
311
メッセージ
18

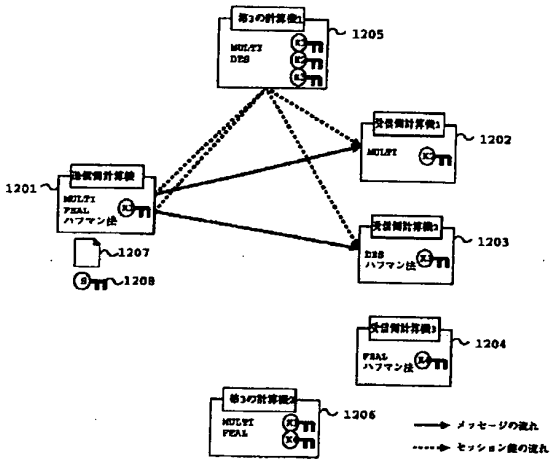
【図１１】

図１１



【図１２】

図１２



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
Ｈ０４Ｌ	9/08		9382－5K	Ｈ０３Ｍ	7/40		
	9/14			Ｈ０４Ｌ	9/00	６０１Ｂ	C-3
// Ｈ０３Ｍ	7/40					６４１	

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内
(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内
(72)発明者　梅木　久志
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内